Chain of Custody

Chain of Custody Explained

The Chain of Custody is a crucial process within computer forensics, and its primary purpose is to ensure that all of the evidence collected in a case has not been tampered with by an unauthorized individual and the original evidence remains unchanged. This involves documenting various information regarding the evidence, such as who, when, and how the evidence was copied or transferred to another person. The Chain of Custody should be maintained from the moment the evidence was collected or acquired to when it is presented at court. As a forensic examiner, you should live and breathe evidence integrity – imagine spending weeks on acquiring and analyzing evidence, only to have it refused to be used as evidence in court because of a lack of Chain of Custody. It's important to understand that the Chain of Custody is important in any criminal investigation, not just digital forensics.

Why is it Important?

The Chain of Custody is extremely important when performing digital forensics for a court case. The court is able to dismiss the evidence if a clear Chain of Custody cannot be presented, as the lack of a Chain of Custody documentation could suggest that there may have been an unauthorized alteration to the evidence. Additionally, the Chain of Custody gives an insight into who handled the evidence, at what time, using what equipment, how it has been tracked (e.g. paper form, spreadsheet), and so on. Essentially, Chain of Custody allows evidence to be tracked and logged, from its acquisition to presentation in court, and thus protects their integrity and security.

FOLLOWING THE CHAIN OF CUSTODY

There are two components to following the Chain of Custody. The first involves ensuring the integrity of the original evidence is maintained. The second involves documenting and recording all of the events that happen to the evidence.

Evidence Integrity Hashing

Before you even think about starting to perform analysis on digital evidence or making a forensic copy of it, or even opening the evidence on your workstation, you should always calculate its hash first. Since hashes are small strings that are unique (with the exception of hash collisions) to the input, they are a quick and easy way to ensure evidence integrity. The hash is calculated before and after handling and compared to confirm that no alterations have been made. The hash does not necessarily have to be cryptographically secure, since it is only used to verify the integrity of the evidence. You should always hash the evidence using at least two methods – the most popular ones being MD5 and SHA1. This is in part due to the possibility (albeit a very low one) of a hash collision attack, where two distinctly different inputs have the same hash value, allowing attackers to modify the evidence without the hash being changed. Alternatively, SHA256 can be used to generate hashes, as they have not caused collisions before.

If the evidence is physical, such as an external hard drive, you should use a hardware write blocker when you connect your workstation to the device. Write blockers only allow the workstation to have read access on the device and blocks any attempts to write to it. Although software options are available, hardware write blockers are the most effective.

Taking a Forensic Copy

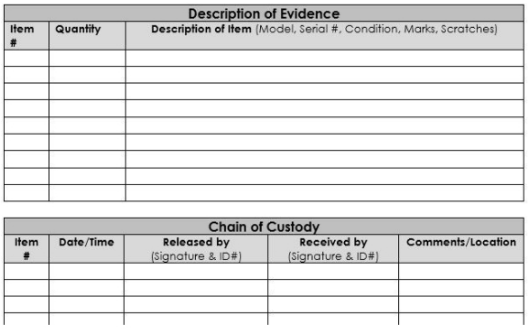
Once the hash of the evidence has been recorded, it is best to make a forensic copy of the original evidence if possible and perform analysis on the copy, as this will allow the original evidence to remain untouched. Many tools are available for this process, from simpler bit-by-bit cloning using the **dd** command in Linux to forensic image generators that automatically add metadata and Chain of Custody information, such as the Forensic Toolkit (FTK) and EnCase.

Storing Digital Evidence

Physical evidence should be stored in antistatic bags which prevent damage through electric discharge to the data it holds. Taking a step further, Faraday cages may be used, which prevents wireless communication and cellular signal exchange of the device within it. In any case, the evidence should be kept within a locked container, which only the authorized examiners have access to and kept within an authorized personnel's watch during transportation.

Chain of Custody Form

Every forensic examiner who works with the evidence should fill out a Chain of Custody form. The form should include the description of the evidence, when/where it has been acquired or transferred, and by whom, the contacts of the examiners, how the evidence has been accessed, collected or stored and other details regarding the evidence. This ensures that there is no broken link within the evidence handling process where the location of the evidence is questioned, as well as having the ability to go back and contact previous examiners.



Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Previous Topic

Mark Complete ✓

Next Topic

Back to Lesson