

**CC SOP-03 - Hard Drive Removal Protocol - Desktop
Computer**

Document ID: 1056
Revision: 1
Effective Date: 8/15/2014
Status: Published
Page 1 of 3

Approved by Director: Dr. Guy Vallaro

A. Purpose:

To outline the steps taken to remove the hard drive(s) from desktop computers that have been submitted to the CCEEL for analysis while maintaining the integrity of the evidence.

B. Responsibility:

CCEEL forensic examiners.

C. Definitions:

Refer to SOP-CC-26 - Definitions and Abbreviations.

D. Procedure:

1. Retrieve the evidence and update the chain of custody.
2. Prepare Imaging Worksheet - Computer (QR-CC-3) for the submitted computer by filling in the Laboratory Case #, Submission #, Start Date and Examiner fields.
3. Prepare Laboratory Notes (QR-CC-5) for the submitted computer by filling in the Laboratory Case #, Submission #, Start Date and Examiner fields.
4. Initial submission barcode label.
5. Use the Laboratory Notes as a narrative to describe actions and observations made during the entire imaging process.
6. Record information on the Imaging Worksheet as it is collected during the course of processing.
7. If submission is packaged, photograph, with a unique identifier present, the unopened package focusing on:
 - a. Evidence labels and any other identifying markers
 - b. Notable marks or damage
8. Remove the packaging.
9. Photograph, with a unique identifier present, the exterior of the computer focusing on:
 - a. Top and front face
 - b. Rear and all connectors
 - c. Serial numbers, evidence labels and any other identifying markers
 - d. Notable marks or damage
10. Record relevant information about the computer in the appropriate fields on the Imaging Worksheet.
11. Open the computer case and note your access into the computer by putting the Laboratory Case Number, Submission Number and your initials on the frame inside the computer.
12. Photograph, with a unique identifier present, the interior of the computer focusing on:
 - a. Overall view of the inside of the computer
 - b. Location of the hard drive(s)

**CC SOP-03 - Hard Drive Removal Protocol - Desktop
Computer**

Document ID: 1056
Revision: 1
Effective Date: 8/15/2014
Status: Published
Page 2 of 3

Approved by Director: Dr. Guy Vallaro

- c. Close-up of the hard drive(s)
 - d. Anything notable inside the case
13. Remove power and data cables, if necessary, from the hard drive(s) and write the following on the cables to indicate the hard drive(s) that the cables were connected to:
- a. Your initials
 - b. Hard drive designator (e.g. "HD1" for hard drive 1, "HD2" for hard drive 2, etc.)
14. Remove hard drive(s) and photograph, with unique identifier present, the hard drive(s) focusing on:
- a. Top of hard drive(s)
 - b. Jumper settings
 - c. Make, model, serial number, LBA and any other identifying markers
15. Note your access to the hard drive(s) with the following information transcribed on the hard drive(s):
- a. Laboratory Case Number
 - b. Sub-item number following the naming convention below:
Evidence Submission Number_Hard Drive Number
For example: S1_HD1.....S1_HD2.....
 - c. Your initials
16. Record relevant information about the hard drive(s) in the appropriate fields on the Imaging Worksheet.
17. Examine the computer's peripheral devices and package for any additional digital media. If additional digital media exists:
- a. Record where the media was located in the Laboratory Notes
 - b. Photograph the digital media with unique identifier present
 - c. Transcribe the following information onto the digital media:
 - i. Laboratory Case Number
 - ii. Sub-item number as outlined in SOP-CC-31 - Sub-item Labeling Standards.
 - iii. Your initials
 - d. Proceed at some point to SOP-CC-6 - Removable Media Imaging Protocol
18. Process the BIOS as follows:
- a. With hard drives removed from the computer connect the computer to a monitor and keyboard
 - b. Turn the computer on
 - c. Break into the setup screens by entering the appropriate keystrokes
 - d. Record the appropriate BIOS information on the Imaging Worksheet

**CC SOP-03 - Hard Drive Removal Protocol - Desktop
Computer**

Document ID: 1056

Revision: 1

Effective Date: 8/15/2014

Status: Published

Page 3 of 3

Approved by Director: Dr. Guy Vallaro

- e. In certain instances it may not be possible to gain access to the BIOS settings. In these cases, document any attempts made and make note in the Laboratory Notes that attempts to access the BIOS were unsuccessful.
- 19. Proceed to SOP-CC-5 – Hard Drive Imaging Protocol and return here upon completion.
- 20. Complete Laboratory Notes and Imaging Worksheet.
- 21. Reassemble the computer leaving the data and power cables disconnected from the hard drive(s).
- 22. Repackage the computer if necessary.
- 23. If additional digital media was found, appropriately package it and adhere it to the computer or place it within the computer's packaging.
- 24. Update the chain of custody in JusticeTrax and return the computer to the evidence area.

ARCHIVED