

Tip Sheet for Forensics Examination

Phil Harrold wrote this.

FORENSIC EXAMINATION PROCEDURAL REVIEW

Note conversations with the person who retained you and what he or she told you.

Describe the media

- what is it
- what color is it
- what size is it
- list any lettering or labeling

Establish a physical chain of custody

- who gave it to you
- write a receipt
- securely store it

How did you get custody of the media

- did you remove it from the computer
- hand delivery
- mail\shipping

How did you protect the media

- write protect
- check the write protect of your machine
- antistatic bag

Establish a hash/crc value of the original media and note it in your report

Wipe and format the media you will be imaging to

Make an image or duplicate

Establish a hash/crc value of the duplicate and note it in your report

Perform the examination on the duplicate\image

Note the volume attributes

- name
- date of format
- what is the OS\filesystem

Note all partitions on the media

-analyze the media partition by partition and file by file

Note all active and deleted files on the media

Establish the path or location of files on the media

Indicate if the file was deleted or not viewable through the OS due to some other action

Recover any documents present and note pertinent content

Recover and note passwords

Analyze document metadata

Analyze internet activity

-browsing history

-temporary internet files

-uploads\downloads

-cookies

-webpage source

Analyze peer to peer or FTP activity

Trace ownership of websites\domains

Note the software used

If you don't have a program, search for trial versions

Note any attempts to conceal or destroy information

Examine slack\unallocated space, look for text, carve out common files

Document all procedures\steps

Draw conclusions about any files that appear to be related

Write a good, professional report and check your spelling