The Case of the Suspect Mole

Activisty Group think that their confidential information is being leaked. Kitten does admin for the group on the computer where this information is kept, and there is suspicion that Kitten is the leak.

You have been asked by the group to look for evidence on the computer that shows whether or not Kitten is leaking confidential group information.

Your task:

You will be provided with a forensic image of the computer.

Perform a digital forensic investigation of this computer to determine any evidence showing whether Kitten or any other party has leaked confidential group information.

Make a report of your investigation; the approach, evidence found, analysis and any conclusions. Be prepared for cross-examination. There is limited time for this investigation.

If practicable, the investigation can progress in two teams;

(a) Investigating for evidence that Kitten is guilty.
(b) Investigating for evidence that Kitten is innocent.

Getting the image

The full computer disk image is supplied on USB flash drive. A ZIP archive of the files is also provided. Hash signatures are included for verifying these copies.

The group also has an open source “Evidence and Case Management System” from which these can be downloaded, at:
http://thebrentc.net/articles/digitalforensics/exercise/

The ZIP archive is simpler to work with and sufficient for this task (to rather use the “raw” image file, you will likely need to apply the booklet section “Mounting a partition within a full disk image”). If unzipping the archive, it’s recommended to sort out a folder for the output files. Generally, you might think about using working copies of evidence.

The USB flash drive is provided in an evidence bag. Tamper-evident bag procedures are: To re-open at *opposite* end from seal, complete reason for opening, process the evidence, then re-seal the evidence and the old bag in a new evidence bag.

Guidance

A strict forensic investigation would use working copies of the full image viewed in read-only mode on a dedicated forensic computer. For the purposes of this exercise, you can take forensic protocols as assumed if you prefer, but note the forensic implications of the approach you take.

The task can be completed using basic skills as described in “Using the command line” in the booklet. Alternatively you could use your computer’s equivalent Graphical User Interface (GUI) file explorer and other programs. You might find the section on Windows 3.11 in the booklet helpful if necessary.

A digital forensic investigation would include taking “contemporaneous notes”. These record the date, time and action taken, made immediately after the action.

The preceding story is fictional and does not depict any actual creature or event.