

## CIS 700 Computer Forensic Laboratory Exercise and Assignment

This 2.5 hour laboratory exercise is intended to introduce you to some of the software tools, processes and procedures that typically are used in a computer forensic investigation.

Your assignment involves producing an expert report based on your observations in the laboratory exercise. This report should be of the caliber and quality of materials that could be presented in court, so some of your grade in this assignment will be based on the appearance of your submission. You should “pretend” that you are working for a forensic laboratory, so you can even make up a logo for the lab that you use on some of the pages of the report so that it looks “official.” The report should be clear, to the point, have no spelling or grammatical errors, and so on. (Suggestion: if you are not a native English speaker, it will probably be helpful to have someone else – NOT someone in this class – look over your report to provide feedback on language.) Do not be afraid to use technical terms in your report (although you should be sure to use them correctly). You do not need to define the technical terms (that would be done by the expert who presents your report in court, or typically a standard glossary of common technical terms would be provided, but please do not do this for the assignment).

Your report will also need to be comprehensive and correct. What you will be doing is known as a “directed search” – since there is never enough time to examine all of the evidence data in any case, decisions are made as to what specific things to look for, generally items that will help the side that you are working for. The senior investigator will work with the attorneys and determine what aspects of the directed search will be performed by the lab investigators. This is often an iterative process, as findings may determine further searches. Often the lab investigators do not know what particular things are being looked for and/or why – all they know is that they are told to collect certain data from the evidence. So, for this project, you should assume that your role is that of a lab investigator. Various tasks are outlined below. Many of these will require that you search for certain information. All of the information that is requested should be provided in your report. There will also be tasks that do not require that information be provided – for these, you should just mention in your report that you performed each task and give a general (very short) description of your observations.

**THIS ASSIGNMENT IS DUE IN HARD (PAPER) COPY FORM BY:**

Monday, August 4, 2008 at 6PM to Dr. Mercuri in order to receive full credit.

This assignment will be accepted through Wednesday, August 6, 2008 at 6PM, but will be docked 1 letter grade (from the grade assigned based on the evaluation of the report).

If there are extenuating circumstances (i.e. REAL, documented, emergencies) that require a late submission, an extension **MAY** be granted but only if you have made a bona fide (documented) attempt to contact Dr. Mercuri **PRIOR** to the time the assignment is due.

For this laboratory exercise you will be working in teams of 2 or 3 students. If you were absent during the laboratory class session, you will have to work by yourself (unless you can find another student, who was also absent, to work with). Each person **MUST** have a chance to do parts of the laboratory – it is **NOT OK** if only one person is the “driver” – so I want to see you taking turns with the various steps (or sub-steps). **IMPORTANT:** *Even though you are working in teams, EACH person must submit an INDIVIDUAL forensic lab report.*

What you will need:

- A. A Helix Boot Disk. This can be created by downloading the .iso file from <http://www.e-fense.com/helix/downloads.php> and burning a bootable disk from the image, or your Professor (or TA) will give you a working Helix disk (in exchange for a blank CD).
- B. A standard PC (Macs will not work) running Windows that can boot from a CD.
- C. Some blank paper to take notes (in forensic work you are often prohibited from bringing any electronic devices into the lab, so paper is often necessary).
- D. A USB thumbdrive (2G or smaller) that you have prepared in advance. The thumbdrive should not contain any files that you would not want others to see, and you should not care if the files are deleted or destroyed. The files should include pictures (of various types, such as .jpg, gif, etc.), directories, text files, and there should also be some files that you had on the thumbdrive and then subsequently deleted.

Steps of the laboratory exercise (do as much of this as you can) – follow the instructions VERY carefully – if you do things in a different sequence than I have them here, or you click on things that you are not supposed to click on, your computer may “hang” and you may need to reboot – if you work methodically and carefully there shouldn’t be trouble:

1. The first page of a forensic report contains details about the forensic examination and is used to authenticate your process and also establish chain of custody. Your first page should include all of the following information: your name and contact information (email address will suffice); the names and of the other “investigators” you are working with (members of your team); the organization you are “working for”; the “matter” that this investigation pertains to; the time, date and location where the examination took place; the computer you used for the examination (look at the back and underside for the brand, model and serial number); the operating system(s) that were used; the software tools that you used; any other equipment or items that you used (give details). For the materials that you examined, give the source of these items (where you got them from, who had them before you). Provide as much of this information as possible, and be as accurate as possible. Handwrite your signature on the front page before you turn the report in (have a printed line for your signature on that page), so it’s “official.”
2. Cold start your computer (turn it on from a power-off state). After you are on the desktop and Windows has stabilized (the hourglass icon has gone away), insert the thumbdrives from your investigative team into the USB slots (if you have more USB drives than slots, you can eliminate the extra drives from the investigation – normally, you’d need to go through all the evidence, but this is just a simulation). Now insert the Helix boot disk into your computer. The Helix disk should start up by itself (be patient, it may take a few seconds) and it will automatically launch the Helix.exe Windows program. If this does not occur, open the “My Computer” icon, and click on the CD drive. This is the “live” version of Helix. (There are actually two DIFFERENT versions of Helix on your boot disk, the other one will be used later in the lab exercise.) When Helix comes up, it will provide a warning – read it (get scared!) and then click on Accept.

3. You are now seeing a Helix menu, which can be accessed using the icons down the left side of the window. We will not be using the Investigative Notes (at the bottom) but you can click on its icon and check it out. We will not be using the documentation (book icon) but you can also check it out (good materials to read later). We probably will not have time to experiment with the tools in the Incident Response area (third icon from the top) but after you finish all of the tasks below, if you have class time left, you can come back to this icon and look at some of its tools.

4. As mentioned before, this is the “live” version of Helix and it is intended to be used if you are starting a forensic exam on a “live” computer. Sometimes when a search warrant is issued, the computers will be found in the “powered on” state. If they are powered off by the police, some very important data may be lost (there may even be booby-traps on the computer that destruct data if it is powered off by someone other than the owner, who knows special procedures to follow). The live version of Helix allows the physical memory (RAM) and the drives to be forensically imaged BEFORE the power is removed from the computer. Generally this is done before doing any other tasks (since other tasks may alter the data). We will not be performing a live acquisition, but you should click on the camera icon and look at the pages there (program that have more than one screen will have a little yellow arrow in the margin of the window, if you click on the arrow you can move through the screens).

5. Now click on the computer icon near the top of the Helix window. The Helix software will collect information about the computer you are using. Copy ALL of this information down, by hand (on paper). This information will go on page 1 of your report. Note: if you inserted the USB drive AFTER you booted Helix, then the USB drive will not show on the System Info screen. You will need to exit Helix (use the x at the upper right corner of the window), take the Helix drive out of the computer, now insert the USB drive, and now put the Helix drive into the computer again, and then click on the Helix computer info icon. Then the USB drive will show. You can do this if you want to see the other USB drives (if you had fewer slots than drives), so that way everyone can check their drives.

6. The next tool you want to use is the one whose icon looks like a file drawer. If you click on that icon, you should get a tree that has the names of your drives (C:, D:, E:, etc.). Try to avoid clicking on C: (for ALL of these exercises, not only this part), since that is your computer hard drive and it (probably) has a LOT of data, so you may be sitting around a LONG time waiting for it to stop. For this lab, you want to investigate one USB thumbdrive (preferably not your own one) and the Helix CD (the Helix CD is probably at D: and the USB drives are probably at E: and F: but you should know which letters are which drives from the data you collected in step 5 (above). If you click on the letter that is the CD drive, you should see 5 items appear on the right panel. These are the files at the top level directory of the CD. The + should appear next to the drive letter. Click on the + and you will see the sub-directories on the CD. Your task is to count up the TOTAL number of files and the total number of directories on the CD, using this tool. (Note: you will need to traverse the directories, open them and count their files and directories.) Check with the members in your team and when you have all decided what you think the answer is, include it in your report. (Don't confer with OTHER teams! If you get the correct answer and they don't, then you will get a better grade!) Then do the

same thing for the thumbdrives. Be sure to identify the thumbdrive with its answer. On each thumbdrive, try to find a picture file (by the extension on the file name). Click on the filename in the right menu. Information about that file should appear in the area below the file list. Copy down all of that information (carefully!). Do this for 2 other files on the thumbdrive of different types (text, etc.). Be sure to include in your notes which thumbdrive you were using. Note: EACH person on your team should collect data on 3 DIFFERENT files.

7. The next-to-bottom icon performs a picture scan of your drive. Click on the icon and then click on “Load Folder” near the bottom of the window. In the “Browse for Folder” pop-up, click on “My Computer.” Then click on the Helix CD icon (in the menu) and click OK. Click OK when it asks you to be patient. The tool will load all of the pictures that it has found on the Helix CD and let you view them. If you SINGLE CLICK on one of the pictures, you will see some information (including the dimension in pixels of the picture) about it near the bottom of the Helix window (do this). If you DOUBLE CLICK on one of the pictures, it will enlarge in a different window, and then you can use the left and right arrows at the bottom of that window to browse through the pictures (do this, and then close that window). Going back to the Helix window, your task is to look at the information for each of the pictures on the Helix disk and determine how many are “thumbnails” and how many are not. A thumbnail (for purposes of this exercise) is defined as a picture whose dimensions are BOTH less than 50. Confer with your team and when you agree on the answer, write it into your notes for your report. Now, click “clear all” at the bottom of the Helix window, and click “load folder” again, and then click on one of the USB thumbdrives and click OK (twice). After the thumbdrive pictures have loaded, see if you can answer this question: “Does this tool load deleted pictures?” Conduct an experiment (using some of the other tools we’ve tried out already) to see if you can determine the answer. Provide an explanation/justification for your answer (not just Yes or No). For this, your team members do not necessarily have to agree, you each should come up with your own justifications (and answer), but you can work together in conducting the experiment.

8. We are now “done” with live Helix, so close its window using the File menu or the x in the corner of the window. When it asks you if you want to save the file log, say no (but this can be helpful in a real investigation).

9. Now you are going to reboot the computer, but this time you are going to boot into the “dead” version of Helix. This version, which runs under Knoppix (Linux), is intended for use when you have a copy of the evidence, since it contains tools that can be destructive to the materials. The easiest way to boot into the other Helix on your CD, from where you are now, is to LEAVE THE HELIX CD IN THE DRIVE. Click on the Start menu, click “turn off computer” and click the “restart” icon (if you accidentally click “turn off” then just wait for it to power off and then press the power on button). If you have clicked “restart” just wait and Windows will shut down and then your system will reboot but this time into Linux from your CD. This may take a while, so be patient! You’ll know that it’s rebooting when you see the word Grub appear on your screen. Next you will see a (different) Helix screen and a menu. Press “enter” on GUI (there are other tools and you can mess with them if you have time after doing all of the required tasks). Helix GUI will

start up (after you see a bunch of Linux command lines on your screen). You will know that Helix GUI is ready when you see the menu bar appear at the bottom of the screen.

10. At the top of your screen should be the various computer (hard and CD). If you have left the thumbdrive(s) in, you should see that (those) too. Over on the left of the menu bar at the bottom of the screen is a tiny Helix icon. Click on that and a menu of tools will appear. There's LOTS of tools here! We will not have time to fool with them, but you can experiment later. The tool we will be using is in the Forensics menu and it is called Retriever. Click on it and a window will open. Slide the window over so you can see the names of your drives. We are going to try to retrieve files from the thumbdrive. Click on Add and then where you see /KNOPPIX/usr/local/... near the top of the window, use the arrow and then click where you see the single "/. Scroll down the menu that appears and click on /media – you should then see the drive names. Click on the name associated with a thumbdrive. Now go to the top part of the screen. Click on the /KNOPPIX/usr/local/... and then click Remove. Only the thumbdrive should be left. Now click on Find (near the bottom of the window). Wait a bit and everything that's ever been on the thumbdrive should appear! Now you can start to have fun! There's a lot of things you can do with this tool. Take turns with members of your group and see what you come up with. The Help isn't very helpful, but there's plenty of information about this tool (and all of the other Helix tools) in the document <http://www.e-fense.com/helix/Docs/Helix0307.pdf> that you can download from the Web. Use one of the computers near you in the Lab that is connected to the Internet, and download this document. Information about the Retriever tool can be found on pages 141-143, or you can just mess around with the tool and try to figure out how it works. See if you can use the tool to find ALL of the picture files on the thumbdrive. Take notes about what you do with the tool and put them in your report.

11. You've now completed all of the required parts of the lab assignment, so this is an opportunity to get some extra credit. Look at the Helix documentation and experiment with 2 more (any two!) of the Helix Linux tools. Write a description of what tools you used, how you used them, and what you were able to find out about the "evidence" on the thumbdrive(s).

12. To end Linux Helix, click on Quit at the bottom of the little Helix icon menu. The CD should pop out. After that happens, press your power off button on the computer until it shuts down (you may have to hold the button longer than usual). **REMEMBER TO REMOVE YOUR THUMBDRIVES!**