# **In this project, you will focus on the architecture and imaging of desktop and laptop computers**

**Learning Goal:**I'm working on a cyber security writing question and need an explanation and answer to help me learn.

Now that you've completed the necessary acquisition and imaging tasks, you're ready to compile all your reports and lab notes into a single forensic imaging lab report that you will submit to your supervisor. Your supervisor reminds you that your report may be presented in a court case, so it needs to meet legal requirements. The report should include the following sections:

1. One- to two-page memo addressing the types, sources, collection of digital information, as well as file formats
2. Imaging of a USB drive using Linux tools (lab notes, report)
3. Imaging of a USB drive using Windows tools (lab notes, report)
4. One- to two-page memo responding to questions about imaging procedures
5. RAM and swap acquisition—live, local computer (lab notes, report)
6. Forensic imaging over a network (lab notes, report)

**Requirements: 4 pages**

Digital forensics involves processing data from many different types of devices, ranging from desktops to laptops, tablets to smartphones, servers to cloud storage, and even devices embedded in automobiles and aircraft. In this project, you will focus on the architecture and imaging of desktop and laptop computers. You will be working in a virtual machine (VM) to image and verify the contents of the following:

* a USB stick
* the random access memory (RAM) and swap space of a live computer
* a networked computer hard drive

There are seven steps in this project. In the first step, you will review a technical manual containing information about where data of forensic value is typically found inside digital devices. The next two steps will guide you through the process of imaging a USB stick with both Linux and Windows tools. The next step will pose several questions that frequently come up in cases similar to this scenario. In the next step, you will be back to collecting forensic evidence; this time you will be imaging the RAM (memory) and swap space of a live, running computer. In the next step, you will image a computer's hard drive over the network. In the final step, you will compile all lab notes and reports into one comprehensive report. The final assignment in this project is a forensic imaging lab report that can be presented in a court of law.

Before you can begin imaging the USB drive provided by your supervisor, you need to review your technical manual in order to prepare a memo to give to your company's legal team. Are you ready to get started?

8 mins ago

**Step 1**

Before you have a chance to begin the imaging process, your supervisor calls to tell you that the organization's legal team has been asking questions about types, sources, and collection of digital information. Team members have also asked about file formats. Your supervisor asks you to prepare a brief explanatory memo. You use the department's technical manual to compose your memo on [finding valuable forensic information](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/finding-valuable-digital-forensic-information.html?ou=610147) and [storing digital evidence](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/storing-digital-evidence.html?ou=610147). You also review [image verification using hashing](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/image-verification-with-hashing.html?ou=610147), an important component of digital forensics.

For the first step in this project, prepare a memo (one to two pages in length [following this format](https://leocontent.umgc.edu/content/dam/course-content/tgs/dfc/dfc-620/document/Memo_Templates_for_Project2.docx?ou=610147)) in plain language that summarizes where valuable digital forensic information resides in the device, as well as collection and storage options. The devices to be addressed are USB sticks, RAM and swap space, and operating system hard disks. You will need to research and cite reference sources for each answer contained your memo (e.g., NIST) For each electronic media device described, include a short description of the following:

* identify the digital media device examined
* types of data that can be found there
* reasons why the data has potential value to an investigation in general, and for this case in particular
* list the possible digital evidence storage formats (raw, E01 (ewf), and AFF) and describe the advantages and disadvantages of each format, and
* how digital forensic images are collected (local and remote, memory and disk) and verified.

Your memo will be included in the final forensic imaging lab report.

7 mins ago

# Step 2: Image a USB Drive Using Linux Tools

In the first step in this project, you reviewed technical information and imaging procedures and briefed your legal team on digital forensic basics. Now, it's time to move forward with the investigation.

The USB stick may contain intellectual property that you can use to prove the suspect's guilt, or at least establish intent. Security personnel recovered the stick from the suspect's desk drawer the night before. You take possession of the stick, recording the physical exchange on the chain-of-custody document prepared by the security officers.

Your team's policy is, when practical, to use multiple tools when conducting digital forensic investigations, so you decide to image the USB stick using both Linux and Windows tools.

To get started, review the lab instructions in the box below, as well as [methods of acquisition](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/methods-of-acquisition.html?ou=610147). Then go to the virtual lab to [set up your evidence drive](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/set-up-your-evidence-drive.html?ou=610147) and proceed to [enable write protection](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/enable-write-protection.html?ou=610147), [sterilize the target media](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/sterilize-the-target-media.html?ou=610147), [perform a static acquisition of Linux data](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/perform-a-static-acquisition-of-linux-data.html?ou=610147), and verify the USB stick on the sterilized media using Linux tools in preparation for the report and notes requested by your supervisor.

6 mins ago

# Step 4: Respond to Questions from the Legal Team

In previous steps, you imaged the USB drive using Linux and Windows tools. In this step, you will create a legal memorandum that responds to pointed questions from your organization's legal team. The legal team has been involved in cybercrime cases before, but team members want to make sure they are prepared for possible legal challenges. They have requested very specific information about imaging procedures based upon your review of reference sources in the field.

Research sources on digital forensics imaging and mounting procedures before writing your response. Then review [Set Up Your Evidence Drive](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/set-up-your-evidence-drive.html?ou=610147), [Hash Functions](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/hash-functions.html?ou=610147), [Imaging Programs](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/imaging-programs.html?ou=610147), and [Image Verification With Hashing](https://leocontent.umgc.edu/content/scor/uncurated/cst/2215-cst640/learning-topic-list/image-verification-with-hashing.html?ou=610147) as needed.

Questions from the legal team:

1. Assuming that this is a criminal case that will be heard in a court of law, which hashing algorithm will you use and why?
2. What if the hash of your original does not match your forensic copy? What kinds of issues could that create? What could cause this situation?
3. What if your OS automatically mounts your flash drive prior to creating your forensic duplicate? What kinds of problems could that create?
4. How will you be able to prove that your OS did not automatically mount your flash drive and change its contents prior to the creation of the forensic copy?

The legal team would like you to respond in the form of a brief memo (one to two pages [following this format](https://leocontent.umgc.edu/content/dam/course-content/tgs/dfc/dfc-620/document/Memo_Templates_for_Project2.docx?ou=610147)) written in plain, simple English. The memo will be included as an attachment to your final forensic imaging lab report in the final step, so review it carefully for accuracy and completeness.

5 mins ago

5 mins ago

Now that you've completed the necessary acquisition and imaging tasks, you're ready to compile all your reports and lab notes into a single forensic imaging lab report that you will submit to your supervisor. Your supervisor reminds you that your report may be presented in a court case, so it needs to meet legal requirements. The report should include the following sections:

1. One- to two-page memo addressing the types, sources, collection of digital information, as well as file formats
2. Imaging of a USB drive using Linux tools (lab notes, report)
3. Imaging of a USB drive using Windows tools (lab notes, report)
4. One- to two-page memo responding to questions about imaging procedures
5. RAM and swap acquisition—live, local computer (lab notes, report)
6. Forensic imaging over a network (lab notes, report)

**do a great job**

Top of Form

Bottom of Form