Lab 1: Getting Prepared for Digital Forensic Programming

Purpose

This lab will help you prepare your environment for digital forensic programming using Python. By the end of this session, you should be able to:

- Use **VS Code** with the integrated terminal.
- Create and activate a **Python virtual environment**.
- Install and verify required packages inside the virtual environment.
- Confirm that **Git** is installed and available.
- Run a simple forensic Python program.

Section A – University Lab Machines (No Admin Rights)

Important Notes

- You **do not have administrator rights** on lab machines.
- All packages must be installed inside the **virtual environment**.
- Do **not** try to install globally — it will fail.
- IT staff have provided a pre-compiled wheel file (`pytsk3-20250312-cp311-cp311-win_amd64.whl`) so you don't need to compile from source.

Step 1 – Check Environment in VS Code Terminal

1. Open **VS Code**.
2. Open the integrated terminal (`Ctrl+`).
3. Run these commands:

```
python --version
pip --version
git --version
```

   - `python` and `pip` must respond with a version.
   - `git` should also respond with a version (if not, Git is not available on this lab machine).

Step 2 – Create a Virtual Environment

1. In VS Code, open the folder where you will store your lab work.
2. Create a virtual environment:

```
python -m venv venv
```

(On macOS, use `python3` instead of `python` if needed.)

3. Activate the virtual environment:
   - **Windows (PowerShell inside VS Code)**:

     ```
     .\venv\Scripts\Activate
     ```

     If you encounter an execution policy error, run the following command to temporarily bypass it, then try activating again:

     ```
     Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
     ```

   - **macOS/Linux**:

     ```
     source venv/bin/activate
     ```

4. Your terminal prompt should now show `(venv)` at the start.

Step 3 – Install Packages from Local Wheel File

Since lab machines cannot compile packages, use the wheel provided by IT staff.

1. Ensure the wheel file (`pytsk3-20250312-cp311-cp311-win_amd64.whl`) is copied into your lab folder.
2. With the virtual environment activated, install using:

   ```
   pip install pytsk3-20250312-cp311-cp311-win_amd64.whl
   ```

   Or, if the file is in another directory, use the full path:

   ```
   pip install "C:\path\to\pytsk3-20250312-cp311-cp311-win_amd64.whl"
   ```

3. Verify installation:

   ```
   pip list
   ```

You should see `pytsk3` listed.

Step 4 – Run the Forensic Program

1. Place the provided file (`demov2.py`) into your lab folder.
2. Run the program:

```
python demov2.py
```

3. The program should display a **menu of forensic options**.

Section B – Personal Laptops (With Admin Rights)

Step 1 – Install Required Software

1. **Visual Studio Code (VS Code)**
   - Download from: https://code.visualstudio.com
   - Install the **Python extension**.
2. **Python 3.11 (Recommended)**
   - The provided wheel file (`pytsk3-20250312-cp311-cp311-win_amd64.whl`) is compiled for Python 3.11 (`cp311`).
   - Download Python 3.11 from: https://www.python.org/downloads/
   - If you use a different Python version, the wheel file may not install correctly.
   - Download from: https://www.python.org/downloads/
   - Tick **Add Python to PATH** during installation.
   - Verify installation:

```
python --version
pip --version
```

3. **Git**
   - Download from: https://git-scm.com/downloads
   - Verify installation:

```
git --version
```

Step 2 – Create and Use a Virtual Environment

Even with admin rights, it is **best practice** to use a virtual environment.

```
python -m venv venv
.\venv\Scripts\Activate      # Windows
source venv/bin/activate     # macOS/Linux
```

Step 3 – Install Packages

You have **two options**:

Option A (Recommended for Consistency – Use Local Wheel File)
If you have been given the same wheel file (`pytsk3-20250312-cp311-cp311-win_amd64.whl`):

```
pip install pytsk3-20250312-cp311-cp311-win_amd64.whl
```

Why use the local wheel file?
Installing `pytsk3` directly from PyPI often fails on Windows because it requires a C++ compiler (such as Microsoft Visual C++ Build Tools) to build the package from source. Most users do not have these build tools installed, and the build process can be complex. The pre-built wheel file avoids this problem by providing a ready-to-install package.

Option B (Install from PyPI – Requires Compiler and Internet)

```
pip install pytsk3
```

Note: If you try this option and see an error like
`error: Microsoft Visual C++ 14.0 or greater is required`,
it means you need to use the local wheel file instead.

Confirm installation with:

```
pip list
```

Step 4 – Run the Forensic Program

Run as before:

```
python demov2.py
```

Student Checklist

For Everyone

- [ ] Open VS Code and terminal.
- [ ] Confirm `python`, `pip`, and `git` are installed.
- [ ] Create and activate a virtual environment.
- [ ] Install `pytsk3` (from **wheel file** or from **PyPI**, depending on setup).
- [ ] Run `pip list` and confirm `pytsk3` is installed.
- [ ] Run `python demov2.py` and confirm the forensic program menu appears.

Additional for Personal Laptops

- [ ] Install VS Code, Python, and Git if not already installed.
- [ ] Ensure **Python is added to PATH** during installation.

Deliverable for Lab 1: Show your instructor that you can:

1. Activate your virtual environment.
2. Run `pip list` and display `pytsk3`.
3. Execute the forensic program (`demov2.py`) and display the menu.