# Connecting a Virtual Machine to AI

MGMT 675: Generative AI for Finance

Kerry Back

# Cowork

# Step 4: Cowork — Claude Acts on Your Files

Claude works autonomously on your local files—you describe the goal, it handles the rest. Switch to the **Cowork** tab in Claude Desktop.

## How it works

1. Point Claude at a folder on your computer
2. Describe the task in plain English
3. Claude plans, writes code, runs it, and delivers results
4. Nothing needs to be installed on your machine—Claude creates a sandboxed workspace automatically

## Example

*"Read portfolio_returns.csv. Calculate the Sharpe ratio for each fund, identify the top 3, and create an Excel file with a summary table and bar chart."*

# What is a Virtual Machine?

# What is a Virtual Machine?

A **virtual machine (VM)** is a computer simulated in software—it has its own operating system, file system, and installed programs, but it runs inside your real computer as an isolated workspace.

## What's Inside the VM

- Linux operating system
- Python (pre-installed)
- Common libraries: `pandas`, `numpy`, `matplotlib`, `openpyxl`, etc.
- Can `pip install` additional packages
- Your files from the folder you selected (mounted into the VM)

## What Makes It "Virtual"

- Created on demand when you start a task
- Runs on your machine, but isolated from your real files and applications
- Temporary—destroyed when the session ends
- Can't accidentally break anything outside the sandbox
- Multiple VMs can run in parallel (sub-agents)

# The Sandbox: What the VM Can and Can't Do

The VM is **sandboxed**—it runs in an isolated environment on your machine with restricted access. This keeps your system safe but limits what Cowork can do.

## Can Do

- Run Python, R, shell scripts
- `pip install` packages
- Read and write files in your selected folder
- Create Excel, Word, PowerPoint, PDF, charts
- Spawn sub-agents for parallel work

## Cannot Do

- **No internet access**—can't call APIs, scrape websites, or fetch live data
- Can't access databases or cloud services
- Can't run GUI applications
- Can't access files outside the selected folder
- Session state lost when the task ends

**Key implication:** Cowork can analyze data you provide, but it cannot fetch new data from the internet. For live API calls, use **Claude Code** instead.

# Comparisons

# Cowork vs. Claude Code

| | **Cowork** | **Claude Code** |
|---|---|---|
| Code runs | In a local VM (sandboxed) | Directly on your machine (no sandbox) |
| Internet access | No | Yes — APIs, databases, web |
| Setup required | None | Python must be installed |
| File access | Selected folder only | Full local file system |
| Sub-agents | Yes (parallel VMs) | Yes (parallel threads) |
| Best for | Non-coders; batch file tasks | Coders; tasks needing live data |
| Token cost | Higher (VM overhead) | Lower (lean context) |

Both are **agentic**—Claude plans and executes autonomously. The difference is *how isolated* the execution is and *what* it can access.

# How Other AI Products Handle Code Execution

Every major AI provider runs code in a sandbox. Cowork is unusual in combining **autonomous planning**, **local file access**, and **parallel sub-agents**.

| | **Claude Cowork** | **ChatGPT Data Analysis** | **Google Colab + Gemini** | **OpenAI Codex** |
|---|---|---|---|---|
| Execution | Local VM | Cloud sandbox | Cloud VM (notebook) | Cloud or local sandbox |
| Internet | Restricted | No | Yes | No (configurable) |
| Local files | Mounted folder | Upload manually | Google Drive | GitHub repo |
| Autonomy | Fully autonomous | Conversational | Hybrid | Autonomous |
| Sub-agents | Yes | No | No | No |
| Focus | General tasks | Data analysis | Notebooks / code | Coding tasks |

# Exercises

# Exercise: Aggregating Diverse Files

- Download loans.zip and extract the files into a folder. You will have a loan tape (CSV), a collateral appraisal report (PDF), and a policy exceptions memo (DOCX).
- In Claude Desktop, go to the Cowork tab and select the folder.
- Ask Claude to read all three files, summarize the key information from each, and produce a single Excel workbook that:
  - Lists every loan with its terms from the CSV
  - Adds a column with the appraised collateral value from the PDF
  - Flags loans that violate the policy limits described in the memo
- Notice that Cowork reads CSV, PDF, and DOCX without any setup on your part—no Python, no file parsing code, no uploads.

# Exercise: Sub-Agents in Action

- Download aggregation.zip and extract the workbooks into a folder.
- In the Cowork tab, select the folder and give Claude this prompt:

*"Each Excel file in this folder contains a data table. Column names vary across files and some columns are missing. For each file independently, summarize the columns present, the number of rows, and basic descriptive statistics. Then combine all files into a single table, reconciling the column names, and save the result as combined.xlsx."*

**Watch the status panel:** Cowork may spawn **sub-agents**—separate workers that analyze individual files in parallel before combining the results. This is the same "divide and conquer" pattern used in professional data pipelines.