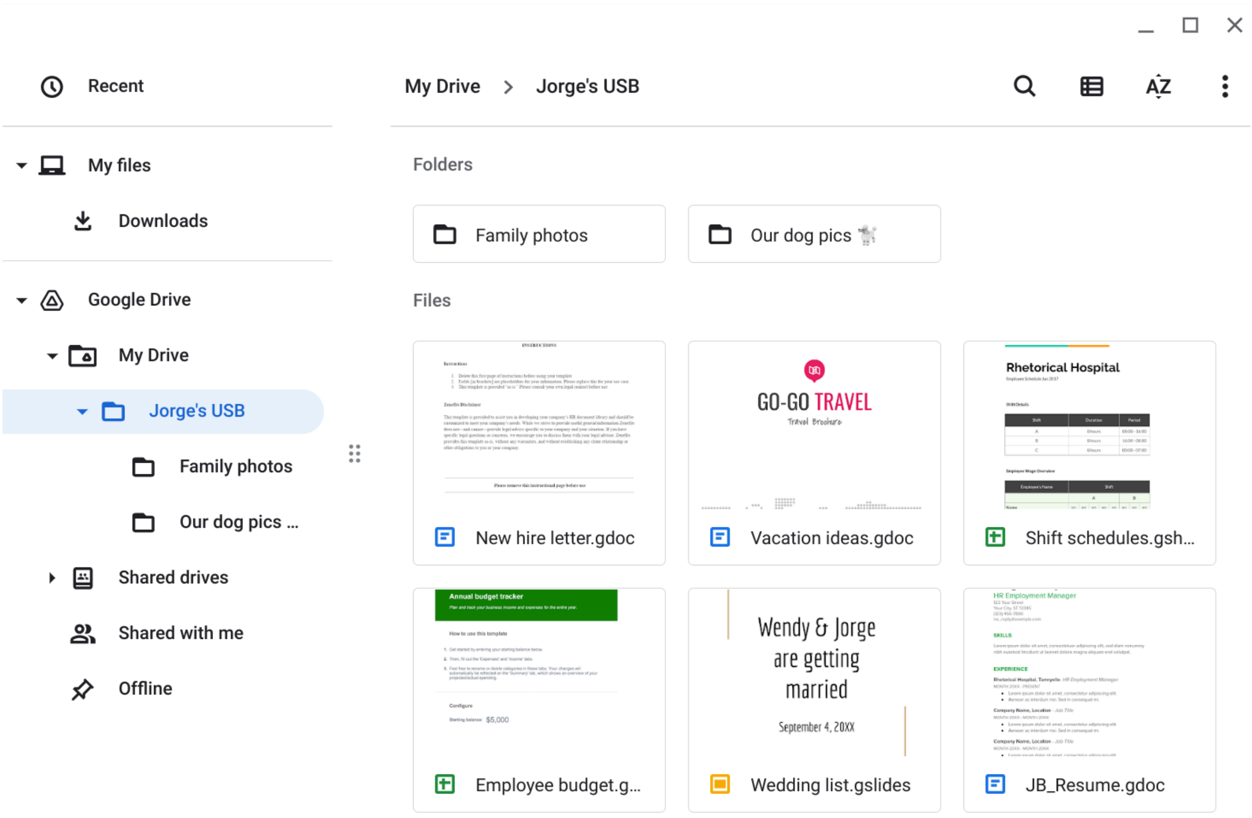
Scenario

You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it's one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn't connected to other files or networks, so the USB drive can't affect other systems if it happens to be infected with malicious software.



Parking lot USB exercise

Contents	This USB drive contains PII which includes the user's resume, wedding plans, family photos, a folder for the user’s dog’s pictures, and vacation ideas. It also contains sensitive work files like an employee budget spreadsheet, shift schedules at the hospital, and a new hire letter.
Attacker mindset	The timesheets that contain employees' shift schedule can provide a hacker insight about other people that Jorge works with and timeslots where they can be vulnerable to even physical attacks outside of work. An attacker can also use an employee's or relative's credentials from the timesheet to bait Jorge with a malicious email designed to look as though it comes from a coworker or relative.
Risk analysis	Raising employee awareness about these types of attacks and how to handle suspicious USB drives is a managerial control that can mitigate the risk of negative incidents. Implementing routine antivirus scans serves as an operational control. Additionally, technical controls should avoid automatically executing malicious code when a USB drive is connected.