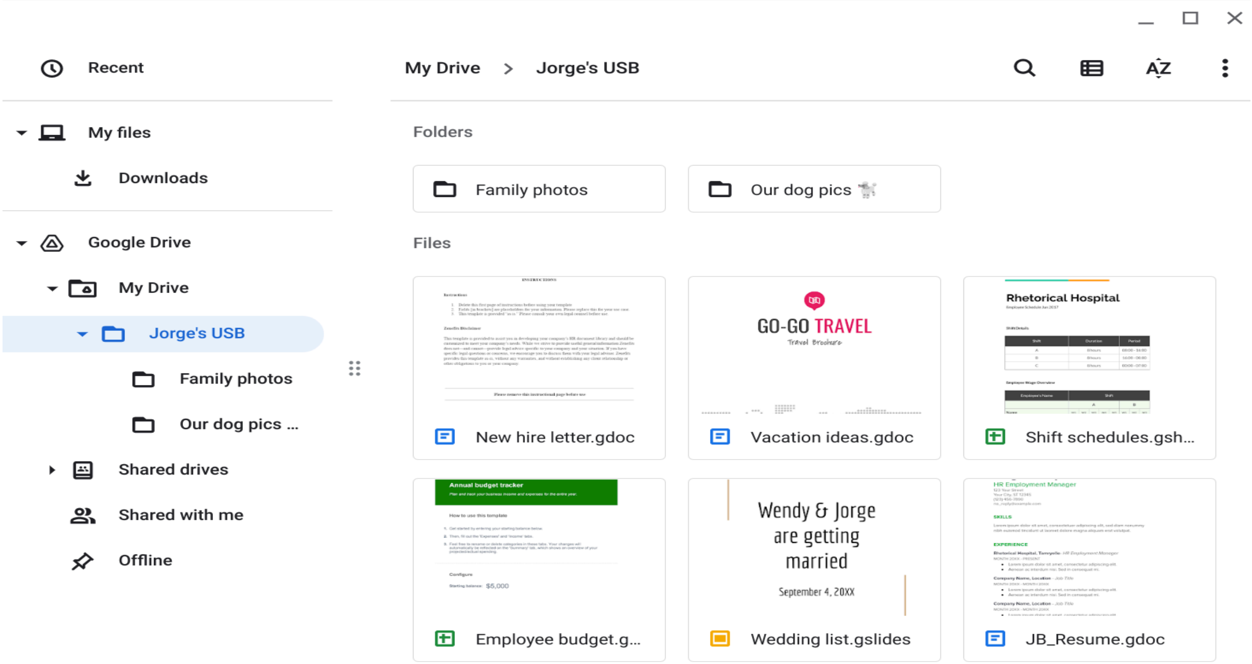
You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who might have dropped it, so you decide to pick it up out of curiosity.
You bring the USB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

You create a virtual environment and plug the USB drive into the workstation. The contents of the device appear to belong to Jorge Bailey, the human resource manager at Rhetorical Hospital.



Parking lot USB exercise

Contents	Jorge’s USB contains some work files (new hire letter, shift schedules, employee budget) and some PII (family photos, wedding list, Resume). The budget tracker likely contains sensitive information of fellow employees. The shift schedule could also be considered sensitive if it were to fall into the hands of someone trying to gain access to the hospital. It is not safe to store work files with personal files.
Attacker mindset	The information on this USB could be used against Jorge’s fellow employees. The employee budget likely contains PII of the employees such as full name, date of birth, ssc, bank account info. The shift schedules could be used by someone trying to gain access to the hospital and want to pretend they were given access to enter areas of the hospital by someone that is on the current shift. If the budget lists which employees work in each department, the attacker could use that information with the shift schedule to pretend they got access permission from someone in IT. This information could also be used against relatives. The attacker could get full names and addresses from the wedding list and try to pair that with family photos to impersonate them on social media. They can use social media to create trust with their targets. Jorge himself could be targeted by a malicious email from someone posing as a fellow employee or relative using the information in these files.
Risk analysis	Malicious software could be hidden on the USB drive and if it were to be plugged into a computer that is connected to the hospitals servers or files an attacker could gain access. PII and potentially SPII could be found on this USB. A sophisticated attacker could use this information to gain access physically or digitally. The hospital should spread awareness to employees to never plug in a suspicious USB and implement controls to make sure no employees store sensitive files on a USB drive. They should also have employees remove any work info from personal computers/files and remove personal information from all work computers/files. The hospital should also routinely scan their systems with antivirus.