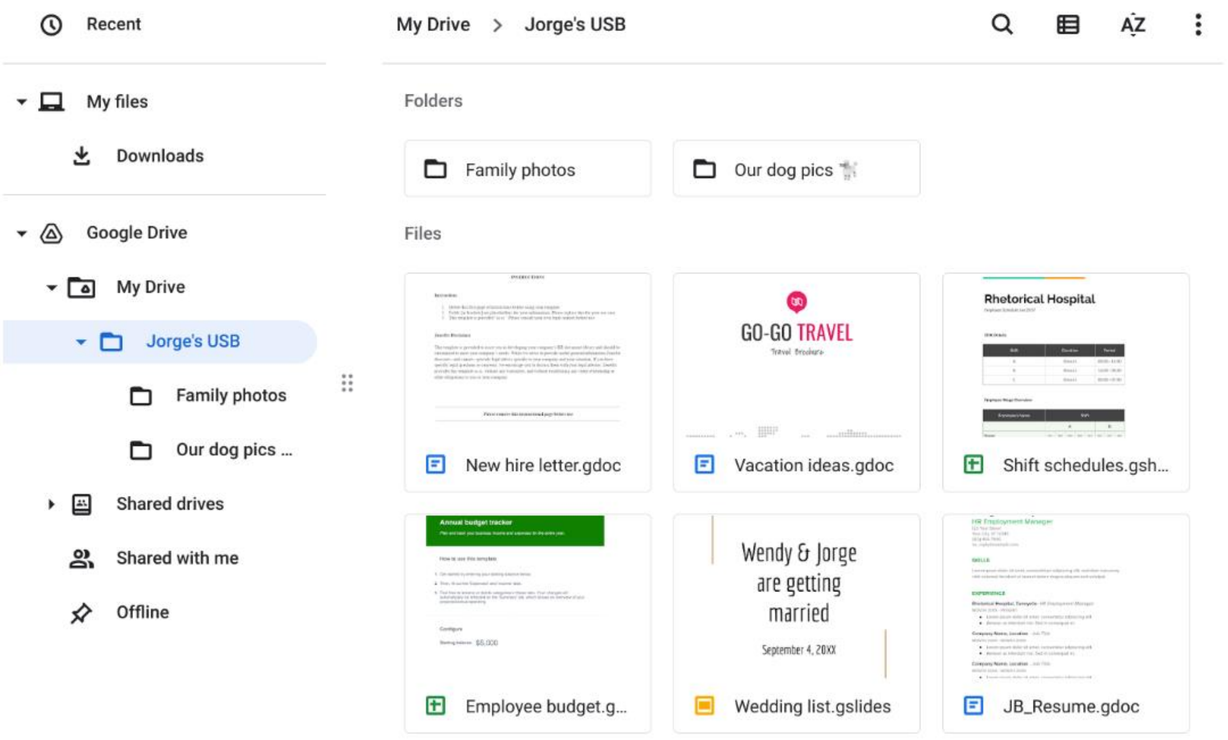
You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who might have dropped it, so you decide to pick it up out of curiosity.

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	There are both work related and personal files on the USB. There is a lot of PII about the owner of the stick, other employees, and the owner of the stock's family/friends. Some examples include a wedding invitation, a resume, a new hire letter, employee budgeting, vacation ideas, and shift schedules.
Attacker mindset	An attacker could use the schedule, employee budget, and new hire letter in multiple ways. They could use the info to phish and social engineer the new hire to obtain PHI, credentials, etc. They could also use the schedule and budgeting form to phish any financial or HR individuals for money, credentials, etc. More on the personal side, the attacker could use the info about the stick owner's resume, family photos, and wedding invitation to phish the marrying couple for money by posing as a vendor or friend. The attack would also take his identity to open accounts, plan trips with family/friends but instead steal money, etc. Depending on how bold the attack is, they could gain access to the building by socially engineering the new hire and knowing the schedule or send detailed phishing emails to the people listed on the schedule. The attacker could just put malicious code on the tick and give it back or leave it back in the parking lot to see if they can gain remote access or more SPII/PHI.
Risk analysis	On USB sticks there could be a lot of malicious software and viruses which can cause damage such as malware, worms, ransomware, remote access tools, credential scrappers, etc. The attacker could have gained access to PII information such as location, addresses, names, emails, phone numbers, etc. Also, depending on what is on the employee budget SPII like credit card numbers/account numbers, etc. Information could be used for phishing, unauthorized access, social engineering, extortion/blackmail, etc.