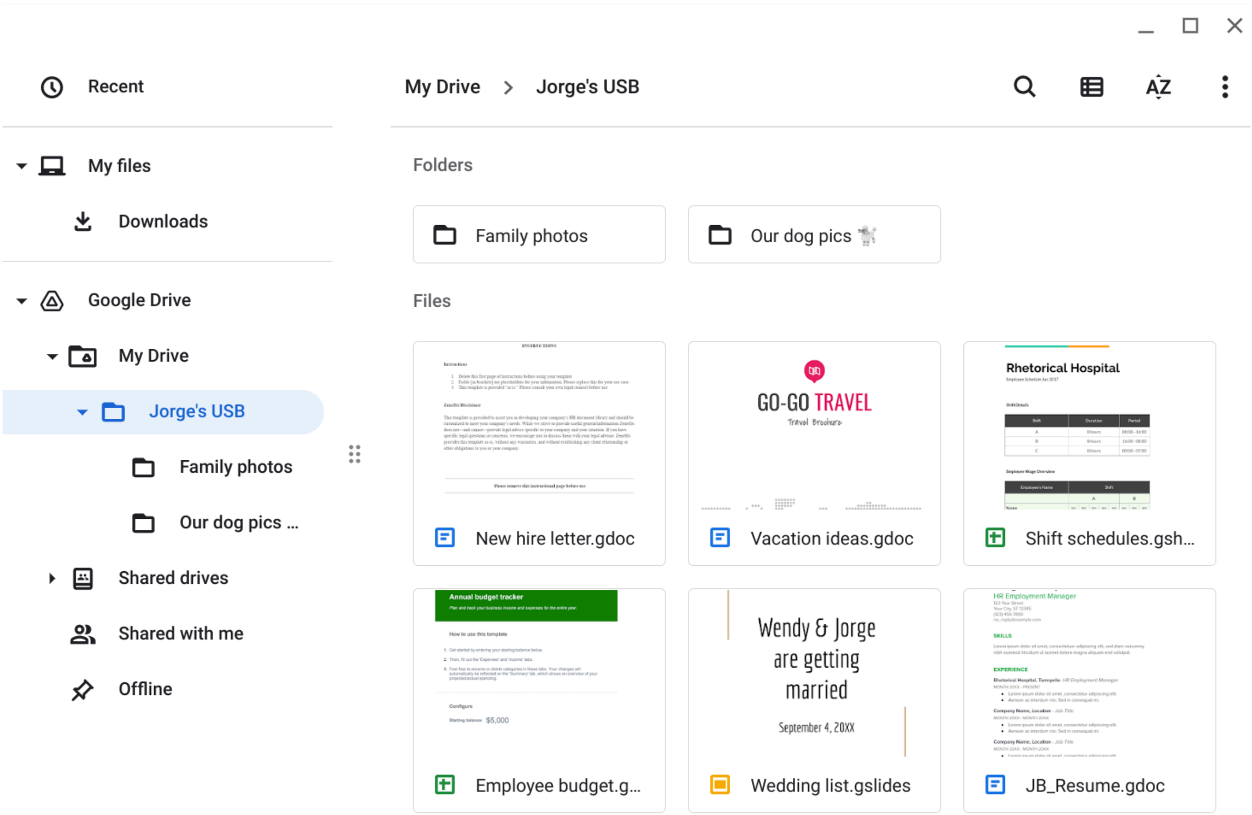
Scenario

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.



Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule.

Review the types of information that Jorge has stored on this device. Then, in the Contents row of the activity template, write 2-3 sentences (40-60 words) about the type of information that's stored on the USB drive.

Parking lot USB exercise

Contents	The USB drive contains a variety of personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. Some of these files may contain Personally Identifiable Information (PII), such as resumes and budget files, which highlights a mix of sensitive and non-sensitive information. It is generally not safe to store personal files alongside work files, especially when sensitive work data is involved, as it increases the risk of data breaches and privacy issues.
Attacker mindset	The information on the USB drive could be exploited to harm Jorge, other employees, or the hospital. Contact details from resumes and sensitive work information like budget data could be used for identity theft or phishing attacks, potentially gaining unauthorized access to secure systems. Additionally, personal photos could be leveraged for social engineering attacks against Jorge's relatives, further compromising security.
Risk analysis	To mitigate these types of attacks, organizations should implement technical controls such as disabling USB ports or using USB port locks to prevent unauthorized use. Additionally, operational controls like regular employee training on the dangers of connecting unknown devices and proper handling procedures for found devices can reduce risks. Managerial controls, including strict data classification policies and access controls, can ensure sensitive information is adequately protected and separated from personal files. Such controls can prevent the spread of malware, safeguard sensitive data, and protect the organization and its employees from potential exploitation.