

# Scenario

13th March 2025

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.

The screenshot shows a Google Drive interface. On the left is a sidebar with navigation options: Recent, My files, Downloads, Google Drive, My Drive, Shared drives, Shared with me, and Offline. The 'My Drive' section is expanded, showing 'Jorge's USB' selected. Below it are 'Family photos' and 'Our dog pics ...'. The main area displays the contents of 'Jorge's USB', which includes two folders and nine files. The folders are 'Family photos' and 'Our dog pics'. The files are: 'New hire letter.gdoc', 'Vacation ideas.gdoc', 'Shift schedules.gsh...', 'Employee budget.g...', 'Wedding list.gslides', and 'JB\_Resume.gdoc'. The 'Shift schedules.gsh...' file is a Google Sheet showing a schedule for Rhetorical Hospital. The 'JB\_Resume.gdoc' file is a resume for Jorge Bailey, HR Employment Manager at Rhetorical Hospital.

Recent

My Drive > Jorge's USB

My files

Downloads

Google Drive

My Drive

Jorge's USB

Family photos

Our dog pics ...

Shared drives

Shared with me

Offline

Folders

Family photos

Our dog pics

Files

New hire letter.gdoc

Vacation ideas.gdoc

Shift schedules.gsh...

Employee budget.g...

Wedding list.gslides

JB\_Resume.gdoc

## Parking lot USB exercise

---

<b>Contents</b>	<i>The files on the USB drive appear to belong to Jorge. The drive contains personal files about Jorge's family and work files which contain intel about the hospital's operations.</i>
<b>Attacker mindset</b>	<i>The intel found on the drive can be used against Jorge since it contains PII; attackers can impersonate the organization and conduct phishing or BEC attacks to gain sensitive data.</i>
<b>Risk analysis</b>	<i>Data in all states should be kept secure. Always, data at rest should be encrypted, this prevents leakage of sensitive information in case of a stolen or missing drive. Additionally, another line of defense can be educating employees on these types of attacks to reduce specific risks.</i>