USB Evidence With USBDeview

Fernando D. Parra

Metropolitan State University of Denver

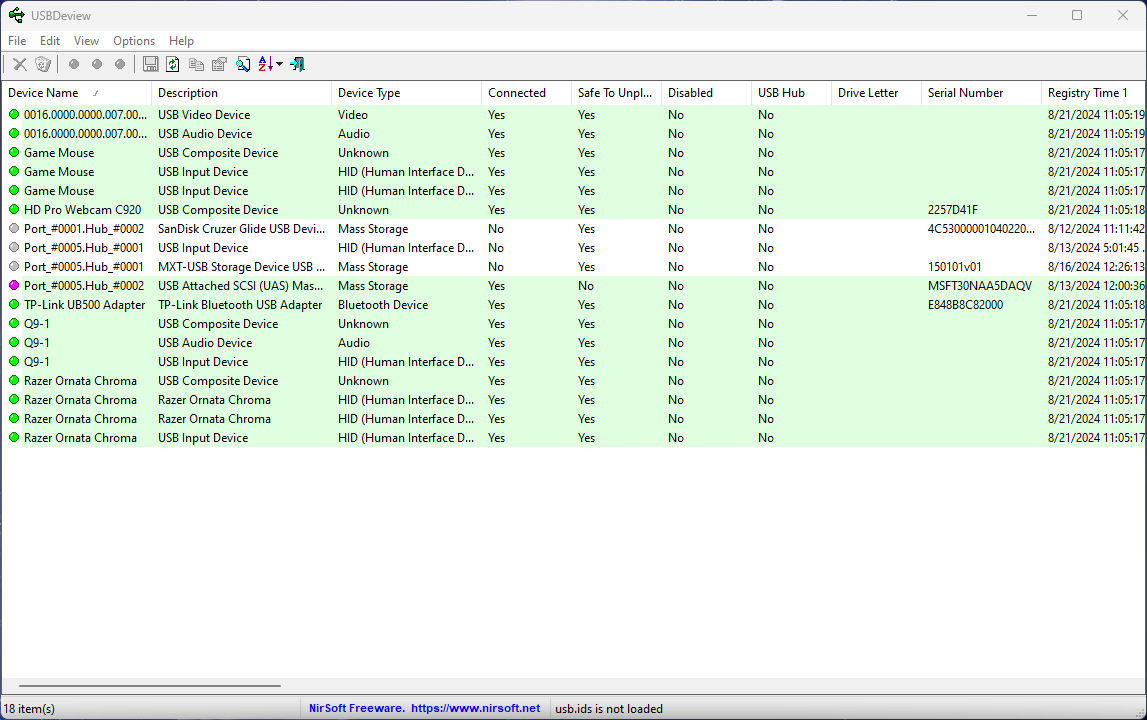
CSS-3652-001 Computer Forensics

Darren R. Hayes

August 28th, 2024

# USB Evidence With USBDeview

Examining the following evidence shows all of the USB HID devices that I’m currently using, like my keyboard (Razer Ornata Chroma), mouse (Game Mouse), Webcam (HD Pro Webcam C920), and USB thumb drives that I’ve previously connected. For instance, the Sandisk Cruzer Glide USB Device assigned as Mass Storage in the Device type column is a bootable USB drive I use to install Linux and Windows OSs like Ubuntu or Windows 11, which I recently switched to. Another interesting finding from the report shows the serial number of a 2 Terabyte portable hard drive currently connected to port number 0005 which can be found using the Device Manager in Windows.



In addition, the report also reveals when (date and time) these devices were connected in the Registry Time 1 column, which is invaluable information in computer forensics investigations. Finally, some attributes worth mentioning from the report are VendorID, ProductID, the current Firmware Revision, the Driver Version, and even the Capabilities of the device/drive.