
From: Bruce Pixley
Sent: Thursday, May 9, 2024 10:18 AM
To: Bill Napier <bill@billnapier.biz>
Subject: RE: Agreement for Forensic Examination of Bell Canyon Computer

On 10/12/2023 at 3:41:04 PM, the laptop hard drive was formatted. Windows was installed on that same day and the "NVR Viewer" user account was created.

The last time the computer was booted was on 10/15/2023 at 9:22:16 PM.

The hard drive is a SK Hynix, model SC311, 256 GB. This is a solid state drive that is commonly shipped with Dell computers. As of now, it appears that this is the original drive that came with the computer.

The formatting and installation of the operating system would overwrite whatever was on the drive in those same sectors. Here is a breakdown of what that looks like:

The primary partition where the operating system, program files, and user data is approximately 236 GB in size. The formatting and installation of the operating system overwrote about 33 GB of data. That overwritten data is unrecoverable.

There is about 203 GB of data (unallocated space) that has not been overwritten.

I have looked at the unallocated space of the solid state drive and it appears to contain random characters. That is odd as normal would be all zeroes as a solid state drive will clean up deleted data with zeroes. The pattern I am seeing is consistent with someone using a wiping tool (prior to the installation of Windows) with a "random generated characters" setting to wipe the drive.

In sum, you have a computer where someone went out of their way to wipe the drive and put a clean install of the operating system on 10/12/2023.

Bruce

Bruce W. Pixley, CISSP, EnCE

From: Bill Napier <bill@billnapier.biz>
Sent: Wednesday, May 8, 2024 12:55 PM