Live Acquisition

This lab will look at how we can acquire RAM from a Windows OS and use the results to find data that could be useful. The data will not always end up at the permanent storage so we have to get it at the time.

We start by logging into the VM and opening the MagnetProcessCapture.exe shortcut either in the folder or on the desktop. We will make sure that all of the svchost processes are check marked in the select processes to capture pane. Then we click select an output folder. We will make a new folder in the evidence repository and name it FOR\_LAB\_002 and make a folder inside it called LAB\_002\_Running\_Processes and hit ok. We verify that the path is correct then hit start and ok at the window pop up. We move back to the desktop and open MRCv120.exe shortcut or find it in the folder, then we hit browse and follow the path to our previous folder, FOR\_LAB\_002 and make a new folder inside called FOR\_LAB\_002\_RAM\_Capture. The file in our new folder is named RAM\_Capture\_Generic\_Desktop\_SN\_954321 and we hit save, change the segment size to 500MB and hit start. Hit ok then close the open windows and delete the folder containing the memory dump RAM\_Capture\_Generic\_Desktop\_SN\_954321.raw located at This PC > Evidence Repository (E:) > LAB\_002 > FOR\_LAB\_002\_RAM\_Capture to make room for the rest of the lab. Now we open accessdata ftk imager either in the folder or on the desktop. Then we hit file, add evidence item, select image file, hit next, browse and follow the path, this pc, desktop, toolbox, datasets, lab2 and choose memdump.mem and hit open then finish. Select memdump.mem and then in the view pane right click and choose fit to window. Now we hit right click find, choose binary hex and type in the box FF D8 FF E0 and hit find. Then we click and hold at the FF D8 top until we get to the FF D9 to select the block then we right click and hit save selection. We save this in the evidence repository for\_lab\_002 folder within a new folder names export and save the file as Mem\_001.jpg and hit save. Moving to the file explorer we follow the path, This PC > Evidence Repository > FOR\_LAB\_002 > RAM\_Capture\_Review > Export and hit right click on our saved file and open with IrfanView 32-bit. Now we close out of everything and open REDLINE in the start menu. Then we click from a saved memory file, hit browse under location of saved memory image and make our way back to the memdump.mem file from before and change file type to all files and hit open, next, and then enter FOR\_Lab\_002\_Redline in the name section and click browse. In the folder we go to our folder in the evidence repository called FOR\_LAB\_002 and make a new folder inside called FOR\_LAB\_002\_Analysis and hit select folder then ok. In the analysis data table, we click processes then we can click on a random process and hit show details. Back at the table, we select drive modules then timeline and look through it before closing the lab.

The lab ran use through several new programs and was interesting to work with as we could see how these new capture processes work and the outcome they provide. The RAM could hold some valuable data that we may not find if you only looked at the permanent storage.

Section 2 Step 8

A screenshot of a computer

Description automatically generated

Section 4 Step 10

A screenshot of a computer

Description automatically generated

Section 5 Step 20

A screenshot of a computer

Description automatically generated

Section 7 Step 18

A screenshot of a computer

Description automatically generated