Questions:

1. Determine the USB devices attached to the system.

USB detector

1. Identify the recently opened PDF documents in the system.

HKEY NTUSER.DAT -> Explorer -> All Files

1. What is the name of computer? {HKLM}

* Doesn’t mean the name of the user
* HKLM
* Load the system registry files
* HKLM -> system -> currControlSet -> control -> ComputerName

DESKTOP-PR…

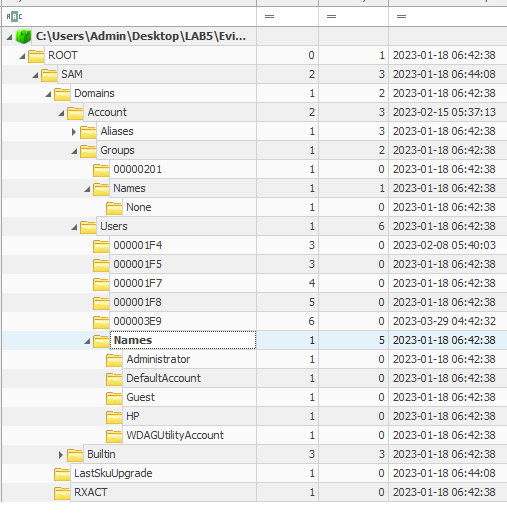
Not Username, its Computer Name

1. What are the user accounts created in the system?

SAM – Security Account Mananger {Stores all the users Related Information}

Hash – NTLM {New Technology Line? Manager}

Names -> …



1. What are the files added to the Start-up location for current logged in user and entire system? {HKCU or HKLM}

NTUSER.DAT/Software

SOFTWARE

1. Identify which virtualization software was used by the current logged in user?

VMWare