Cyber Law and Forensics (CS402)

Lab Assignment 5

**U19CS012**

A.) Answer the Following Questions from the Given Evidence Files:

(1) Determine the **USB devices** attached to the system.

**Tool Used**:

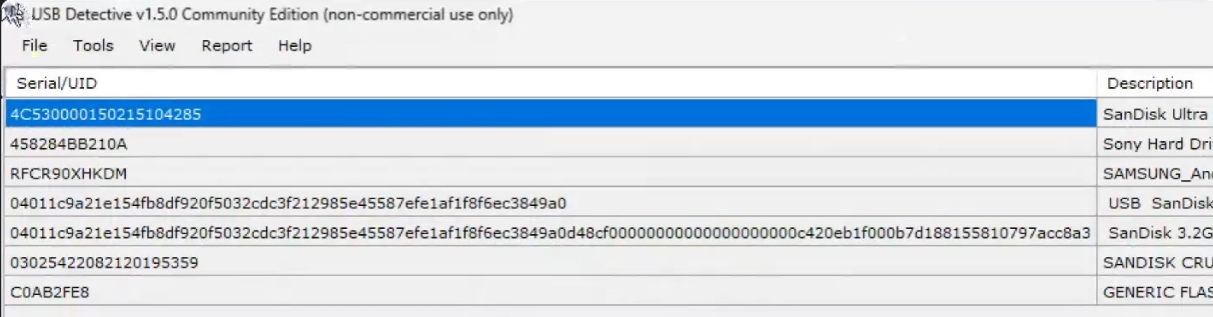
Offline Condition -> USB Detective

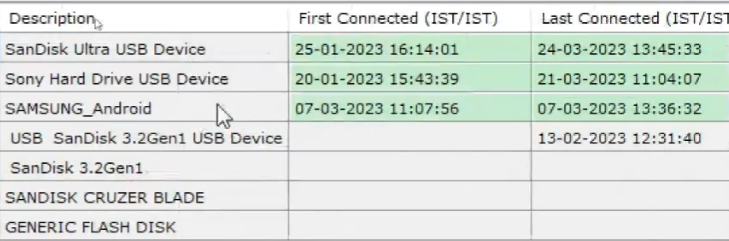
Online Condition -> Tools like USDdeview (working Copy)

**File Used**:

1. SYSTEM Hive
2. SOFTWARE Hive
3. NTUSER.DAT Hive
4. Setupapi Log
5. Amcache Hive

Above Files were extracted using FTK Imager.





Answer -

SanDisk Ultra USB Device

Sony Hard Drive IJSB Device

SAMSUNG\_Android

USB SanDisk 3.2Gen1 USB Device

SanDisk 3.2Gen1

SANDISK CRUZER BLADE

GENERIC FLASH DISK

(2) Identify the recently opened PDF documents in the system.

Remember, the Registry Key “**recentdocs**”, based on extension “**.pdf**” .

**Tool Used**:

Registry Explorer by Eric Zimmerman

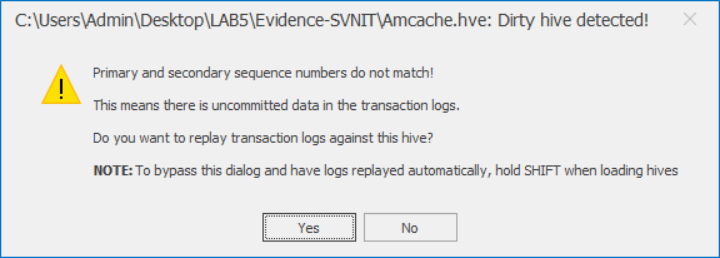
**File Used**:

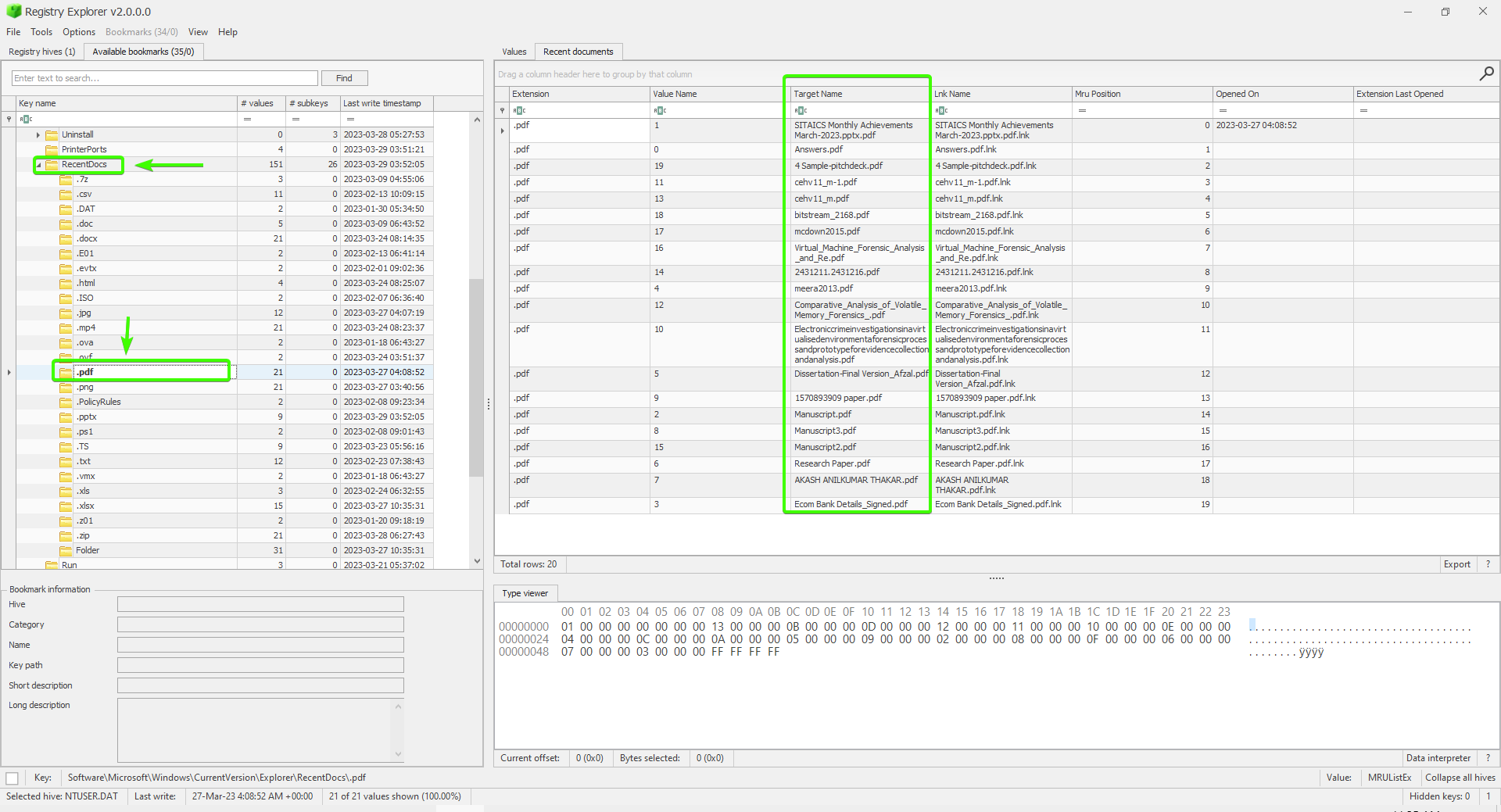
NTUSER.DAT

**Process followed**:

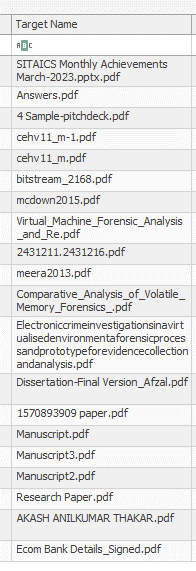
a.) Install the [Registry Explorer Tool](https://ericzimmerman.github.io/) by Eric Zimmerman

b.) Load the “NTUSER.DAT” in Registry Explorer (Select **No** -> Then **Yes** in Next Dialog Popup)





Answer -



**Path**:

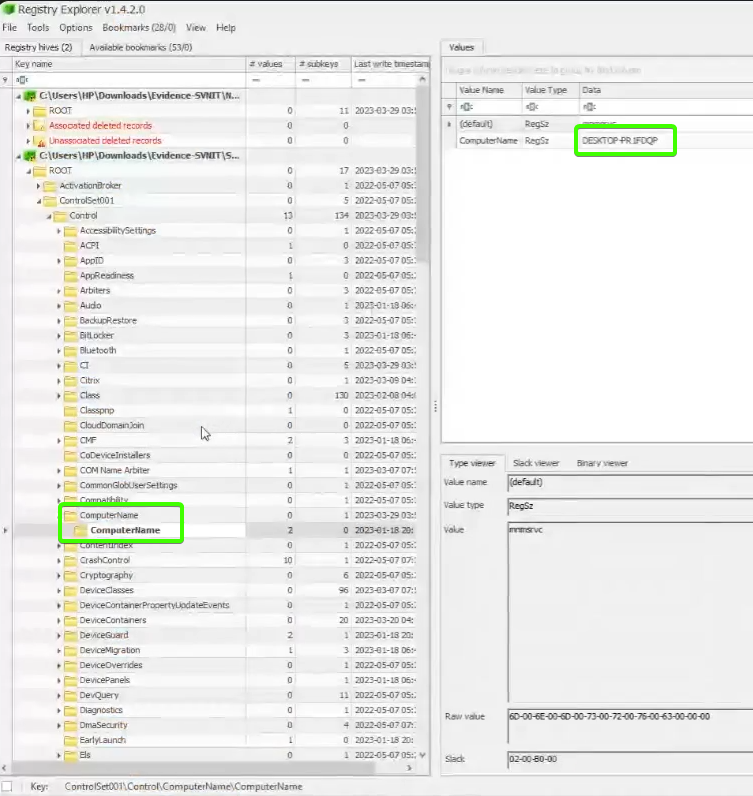
System (HKLM) \ Software \ Microsoft \ Windows \ Current Version \ RecentDocs

(3) What is the name of computer? – “**DESKTOP-PR1FDQP**”

Username is different from Computer Name (Not User Specific, System Specific [HKLM]).

**Tool Used**: Registry Explorer by Eric Zimmerman

**File Used**: NTUSER.DAT



Path: ControlSet001 \ Control \ ComputerName \ ComputerName

(4) What are the user accounts created in the system?

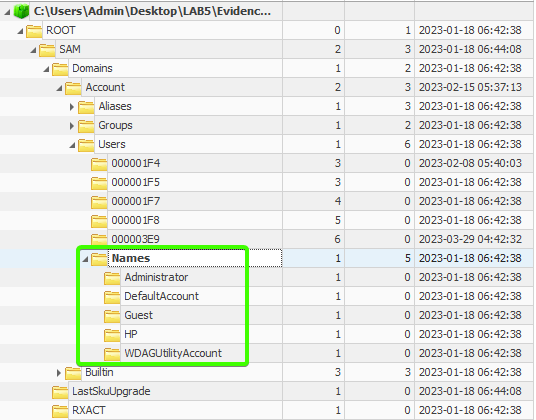
* SAM (Security Account Manager) – Stores user related Information (Password is Stored in NTLM Hash{New Technology LAN Manager})
* SAM is located C: \ Windows \ System32 \ config \ SAM

**Tool Used**:

Registry Explorer by Eric Zimmerman

**File Used**:

SAM



**Path**: SAM\Domains\Account\Users\Names

(5) What are the files added to the Start-up location for **current logged** in user and entire system?

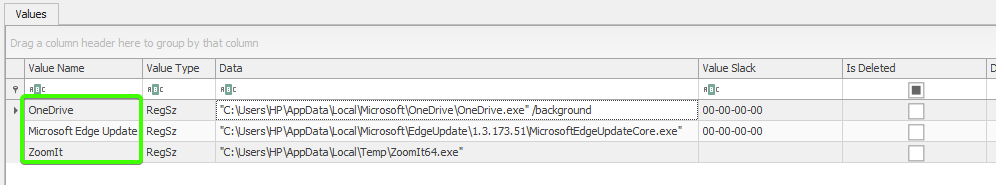
5.a) Files added for current logged in user

**Tool Used**:

Registry Explorer by Eric Zimmerman

**File Used**:

NTUSER.DAT



**Path**:

Software\Microsoft\Windows\CurrentVersion\Run

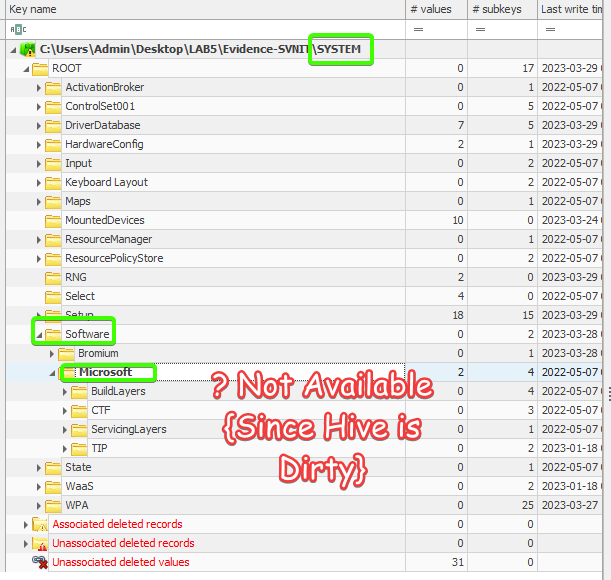
5.b) Files added for Entire System

**Tool Used**:

Registry Explorer by Eric Zimmerman

**File Used**:

SYSTEM



Dirty Hive – System related Files have been deleted.

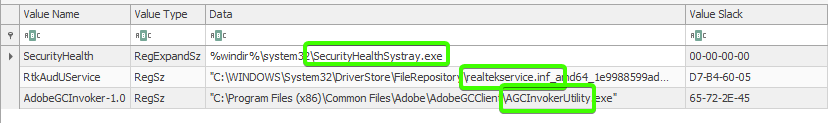
**Path**:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Not Found in HKLM, So Checking with **SOFTWARE** Hive.

**File Used**:

SOFTWARE

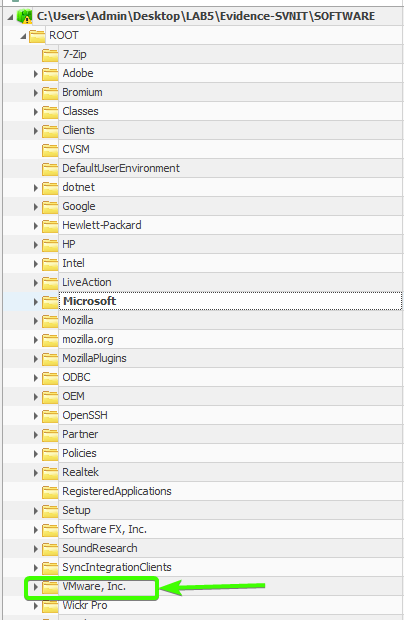


Above 3 Software’s will start for Entire System.

**Path**:

Microsoft\Windows\CurrentVersion\Run

(6) Identify which **virtualization software** was used by the current logged in user? – “VMWare”



**Path**: Microsoft

**SUBMITTED BY**:

U19CS012

BHAGYA VINOD RANA