

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 USDdevview (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.

USB Detective v1.5.0 Community Edition (non-commercial use only)	
File Tools View Report Help	
Serial/UID	Description
4C530000150215104285	SanDisk Ultra
458284BB210A	Sony Hard Dri
RFCR90XHKDM	SAMSUNG_An
04011c9a21e154fb8df920f5032cdc3f212985e45587efe1af1f8f6ec3849a0	USB SanDisk
04011c9a21e154fb8df920f5032cdc3f212985e45587efe1af1f8f6ec3849a0d48cf00000000000000000c420eb1f000b7d188155810797acc8a3	SanDisk 3.2G
03025422082120195359	SANDISK CRU
C0AB2FE8	GENERIC FLAS

Description	First Connected (IST/IST)	Last Connected (IST/IST)
SanDisk Ultra USB Device	25-01-2023 16:14:01	24-03-2023 13:45:33
Sony Hard Drive USB Device	20-01-2023 15:43:39	21-03-2023 11:04:07
SAMSUNG_Android	07-03-2023 11:07:56	07-03-2023 13:36:32
USB SanDisk 3.2Gen1 USB Device		13-02-2023 12:31:40
SanDisk 3.2Gen1		
SANDISK CRUZER BLADE		
GENERIC FLASH DISK		

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

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (34/0) View Help

Registry hives (1) Available bookmarks (15/0)

Enter text to search... Find

Key name # values # subkeys Last write timestamp

Uninstall

PrinterPorts

RecentDocs

7z

csv

.DAT

.doc

.docx

.ED1

.evtx

.html

.ISO

.jpg

.mp4

.ova

.pdf

.png

PolicyRules

.rptx

.xml

.TS

.txt

.vmx

.xls

.xlsx

.x01

.Folder

Run

0

151

3

11

2

21

2

21

2

4

2

12

21

2

21

2

9

12

2

15

21

31

3

26

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

2023-03-28 05:27:53

0 2023-03-29 03:51:21

0 2023-03-29 03:50:05

0 2023-03-09 04:55:06

0 2023-02-13 10:09:15

0 2023-01-30 05:34:50

0 2023-03-09 06:43:52

0 2023-03-24 08:14:35

0 2023-02-13 06:41:14

0 2023-02-01 09:02:36

0 2023-03-24 08:25:07

0 2023-02-07 06:36:40

0 2023-03-27 04:07:19

0 2023-03-24 08:23:37

0 2023-01-18 06:43:27

0 2023-03-24 03:51:37

0 2023-03-27 04:08:52

0 2023-03-27 03:40:56

0 2023-02-08 09:23:34

0 2023-02-03 03:50:05

0 2023-02-08 09:14:43

0 2023-03-23 05:56:16

0 2023-02-23 07:38:43

0 2023-01-18 06:43:27

0 2023-02-06 32:55

0 2023-03-27 10:35:31

0 2023-01-30 09:18:19

0 2023-03-26 06:27:43

0 2023-03-27 10:35:31

0 2023-03-21 05:37:02

Bookmark information

Hive

Category

Name

Key path

Short description

Long description

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.pdf

Selected hive: NTUSER.DAT Last write: 27-Mar-23 4:08:52 AM +00:00 21 of 21 values shown (100.00%)

Values Recent documents

Drag a column header here to group by this column

Extension	Value Name	Target Name	Link Name	Mru Position	Opened On	Extension Last Opened
.pdf	1	SITAICS Monthly Achievements March-2023.pptx.pdf	SITAICS Monthly Achievements March-2023.pptx.pdf.link	0	2023-03-27 04:08:52	
.pdf	0	Answers.pdf	Answers.pdf.link	1		
.pdf	19	4 Sample-pitchdeck.pdf	4 Sample-pitchdeck.pdf.link	2		
.pdf	11	cehv11_m-1.pdf	cehv11_m-1.pdf.link	3		
.pdf	13	cehv11_m.pdf	cehv11_m.pdf.link	4		
.pdf	18	bitstream_2168.pdf	bitstream_2168.pdf.link	5		
.pdf	17	midswon2015.pdf	midswon2015.pdf.link	6		
.pdf	16	Virtual_Machine_Forensic_Analysis_and_Re.pdf	Virtual_Machine_Forensic_Analysis_and_Re.pdf.link	7		
.pdf	14	2431211_2431216.pdf	2431211_2431216.pdf.link	8		
.pdf	4	meera2013.pdf	meera2013.pdf.link	9		
.pdf	12	Comparative_Analysis_of_Volatile_Memory_Forensics.pdf	Comparative_Analysis_of_Volatile_Memory_Forensics.pdf.link	10		
.pdf	10	ElectronicInvestigationsinaviatualisedenvironmentforforensicsprossandrobitypoforensicevidencecollectionandanalysis.pdf	ElectronicInvestigationsinaviatualisedenvironmentforforensicsprossandrobitypoforensicevidencecollectionandanalysis.pdf.link	11		
.pdf	5	Dissertation-Final Version_Afzal.pdf	Dissertation-Final Version_Afzal.pdf.link	12		
.pdf	9	1570892909 paper.pdf	1570892909 paper.pdf.link	13		
.pdf	2	Manuscript.pdf	Manuscript.pdf.link	14		
.pdf	8	Manuscript3.pdf	Manuscript3.pdf.link	15		
.pdf	15	Manuscript2.pdf	Manuscript2.pdf.link	16		
.pdf	6	Research Paper.pdf	Research Paper.pdf.link	17		
.pdf	7	AKASH ANILKUMAR THAKAR.pdf	AKASH ANILKUMAR THAKAR.pdf.link	18		
.pdf	3	Ecom Bank Details_Signed.pdf	Ecom Bank Details_Signed.pdf.link	19		

Total rows: 20 Export ?

.....

Type viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23

00000000 00 00 00 00 00 00 00 00 13 00

00000024 04 00 00 00 00 00 00 0A 00

00000048 07 00 00 00 03 00 00 00 FF FF FF FF

.....

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Data interpreter ?

Value MRUListx Collapse all hides

Hidden keys: 0

Answer -

Target Name
Microsoft
SITAICS Monthly Achievements March-2023.pptx.pdf
Answers.pdf
4 Sample-pitchdeck.pdf
cehv11_m-1.pdf
cehv11_m.pdf
bitstream_2168.pdf
mcdowd2015.pdf
Virtual_Machine_Forensic_Analysis _and_Re.pdf
2431211.2431216.pdf
meera2013.pdf
Comparative_Analysis_of_Volatile_ Memory_Forensics_.pdf
Electroniccrimeinvestigationinavirt ualisedenvironmentaforensicproces sandprototypeforevidencecollection andanalysis.pdf
Dissertation-Final Version_Afzal.pdf
1570893909 paper.pdf
Manuscript.pdf
Manuscript3.pdf
Manuscript2.pdf
Research Paper.pdf
AKASH ANILKUMAR THAKAR.pdf
Ecom Bank Details_Signed.pdf

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

Registry Explorer v1.4.2.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (2) Available bookmarks (53/0)

Key name	# values	# subkeys	Last write timestamp
C:\Users\HP\Downloads\Evidence-SVMT\N...	0	11	2023-03-29 03:1
ROOT	0	0	
Associated deleted records	0	0	
Unassociated deleted records	0	0	
C:\Users\HP\Downloads\Evidence-SVMT\S...	0	17	2023-03-29 03:1
ROOT	0	1	2022-05-07 05:1
ActivationBroker	0	5	2022-05-07 05:1
ControlSet001	13	134	2023-03-29 03:1
Control	0	1	2022-05-07 05:1
AccessibilitySettings	1	0	2022-05-07 05:1
ACPI	0	3	2022-05-07 05:1
AppID	1	0	2022-05-07 05:1
AppReadiness	0	3	2022-05-07 05:1
Arbiters	0	1	2023-01-18 06:1
Audio	0	3	2022-05-07 05:1
BackupRestore	0	3	2023-01-18 06:1
BitLocker	0	1	2022-05-07 05:1
Bluetooth	0	5	2023-03-29 03:1
CT	0	1	2023-03-09 04:1
Citrix	0	130	2022-05-07 05:1
Class	1	0	2022-05-07 05:1
Classprep	0	3	2022-05-07 05:1
CloudDomainJoin	2	3	2023-01-18 06:1
CMF	0	1	2022-05-07 05:1
CoDeviceInstallers	1	1	2022-05-07 05:1
COM Name Arbitrator	0	1	2022-05-07 05:1
CommonGlobUserSettings	0	1	2022-05-07 05:1
Compatibility	0	1	2023-03-29 03:1
ComputerName	2	0	2023-01-18 20:1
ContentIndex	10	1	2022-05-07 07:1
CrashControl	0	6	2022-05-07 05:1
Cryptography	0	96	2023-03-07 07:1
DeviceClasses	0	1	2022-05-07 05:1
DeviceContainerPropertyUpdateEvents	0	20	2023-03-20 04:1
DeviceContainers	2	1	2023-01-18 20:1
DeviceGuard	3	1	2023-01-18 06:1
DeviceMigration	0	1	2022-05-07 05:1
DeviceOverrides	0	1	2023-01-18 06:1
DevicePanels	0	11	2022-05-07 05:1
DevQuery	0	1	2022-05-07 07:1
Diagnostics	4	0	2023-01-18 20:1
DmaSecurity	1	1	2022-05-07 05:1
EarlyLaunch	0	1	2022-05-07 05:1
Eis	0		

Values

Value Name	Value Type	Data
(default)	RegSz	mmtrvc
ComputerName	RegSz	DESKTOP-PR1FDQP

Type viewer

Value name	Value type	Value
(default)	RegSz	mmtrvc

Raw value

60-00-6E-00-6D-00-73-00-72-00-76-00-63-00-00-00

Slack

02-00-80-00

Key: ControlSet001\Control\ComputerName\ComputerName

Path: ControlSet001 \ Control \ ComputerName \ ComputerName

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

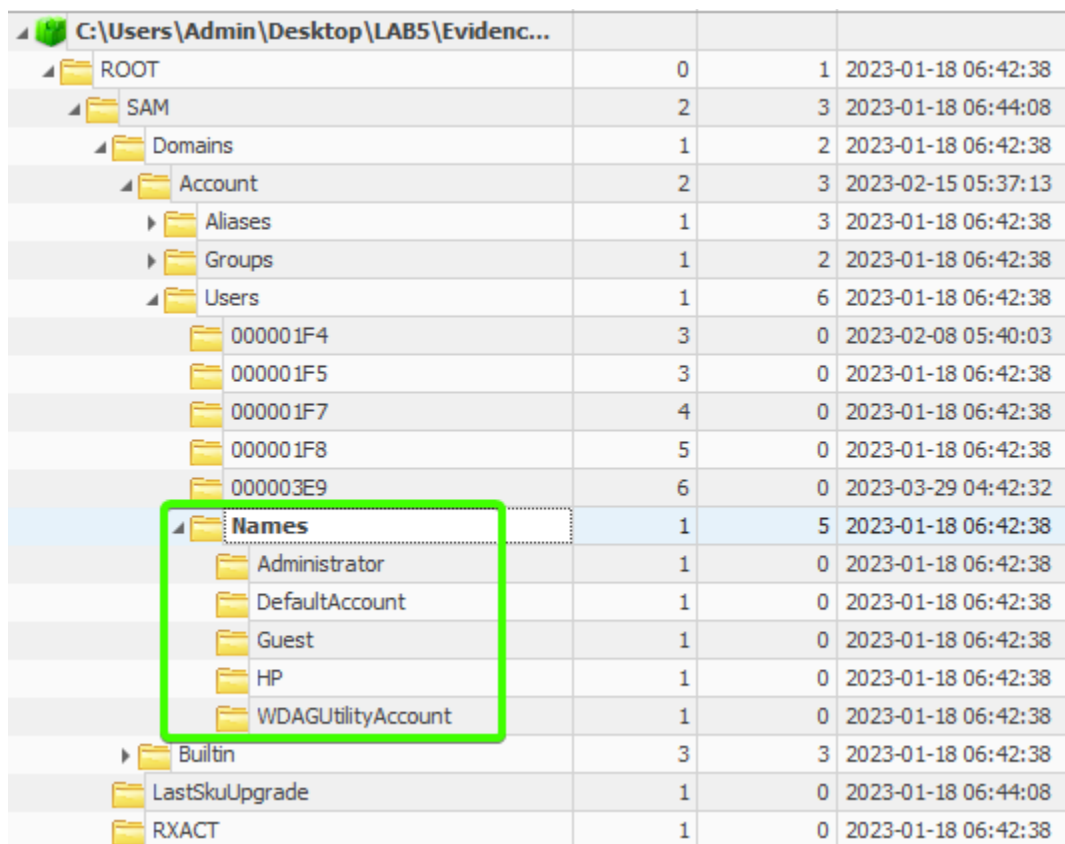
- ✓ SAM (Security Account Manager) - Stores user related Information (Password is Stored in NTLM Hash{New Technology LAN Manager})
- ✓ SAM is located C: \ Windows \ System32 \ config \ SAM

Tool Used:

Registry Explorer by Eric Zimmerman

File Used:

SAM



ROOT	0	1	2023-01-18 06:42:38
SAM	2	3	2023-01-18 06:44:08
Domains	1	2	2023-01-18 06:42:38
Account	2	3	2023-02-15 05:37:13
Aliases	1	3	2023-01-18 06:42:38
Groups	1	2	2023-01-18 06:42:38
Users	1	6	2023-01-18 06:42:38
000001F4	3	0	2023-02-08 05:40:03
000001F5	3	0	2023-01-18 06:42:38
000001F7	4	0	2023-01-18 06:42:38
000001F8	5	0	2023-01-18 06:42:38
000003E9	6	0	2023-03-29 04:42:32
Names	1	5	2023-01-18 06:42:38
Administrator	1	0	2023-01-18 06:42:38
DefaultAccount	1	0	2023-01-18 06:42:38
Guest	1	0	2023-01-18 06:42:38
HP	1	0	2023-01-18 06:42:38
WDAGUtilityAccount	1	0	2023-01-18 06:42:38
Builtin	3	3	2023-01-18 06:42:38
LastSkuUpgrade	1	0	2023-01-18 06:44:08
RXACT	1	0	2023-01-18 06:42:38

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

Values					
Drag a column header here to group by that column					
	Value Name	Value Type	Data	Value Slack	Is Deleted
▼	#c	#c	#c	#c	<input checked="" type="checkbox"/>
▶	OneDrive	RegSz	"C:\Users\HP\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	00-00-00-00	<input type="checkbox"/>
	Microsoft Edge Update	RegSz	"C:\Users\HP\AppData\Local\Microsoft\EdgeUpdate\1.3.173.51\MicrosoftEdgeUpdateCore.exe"	00-00-00-00	<input type="checkbox"/>
	ZoomIt	RegSz	"C:\Users\HP\AppData\Local\Temp\ZoomIt64.exe"		<input type="checkbox"/>

Path:

Software\Microsoft\Windows\CurrentVersion\Run

5.b) Files added for Entire System

Tool Used:

Registry Explorer by Eric Zimmerman

File Used:

SYSTEM

Key name	# values	# subkeys	Last write time
C:\Users\Admin\Desktop\LAB5\Evidence-SVMT\SYSTEM	=	=	=
ROOT	0	17	2023-03-29
ActivationBroker	0	1	2022-05-07
ControlSet001	0	5	2022-05-07
DriverDatabase	7	5	2023-03-29
HardwareConfig	2	1	2023-03-29
Input	0	2	2022-05-07
Keyboard Layout	0	2	2022-05-07
Maps	0	1	2022-05-07
MountedDevices	10	0	2023-03-24
ResourceManager	0	1	2022-05-07
ResourcePolicyStore	0	2	2022-05-07
RNG	2	0	2023-03-29
Select	4	0	2022-05-07
Setup	18	15	2023-03-29
Software	0	2	2023-03-28
Bromium	0	1	2023-03-28
Microsoft	2	4	2022-05-07
BuildLayers	0	4	2022-05-07
CTF	0	3	2022-05-07
ServicingLayers	0	1	2022-05-07
TIP	0	2	2023-01-18
State	0	1	2022-05-07
WaaS	0	2	2023-01-18
WPA	0	25	2023-03-27
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	31	0	

? Not Available
{Since Hive is
Dirty}

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

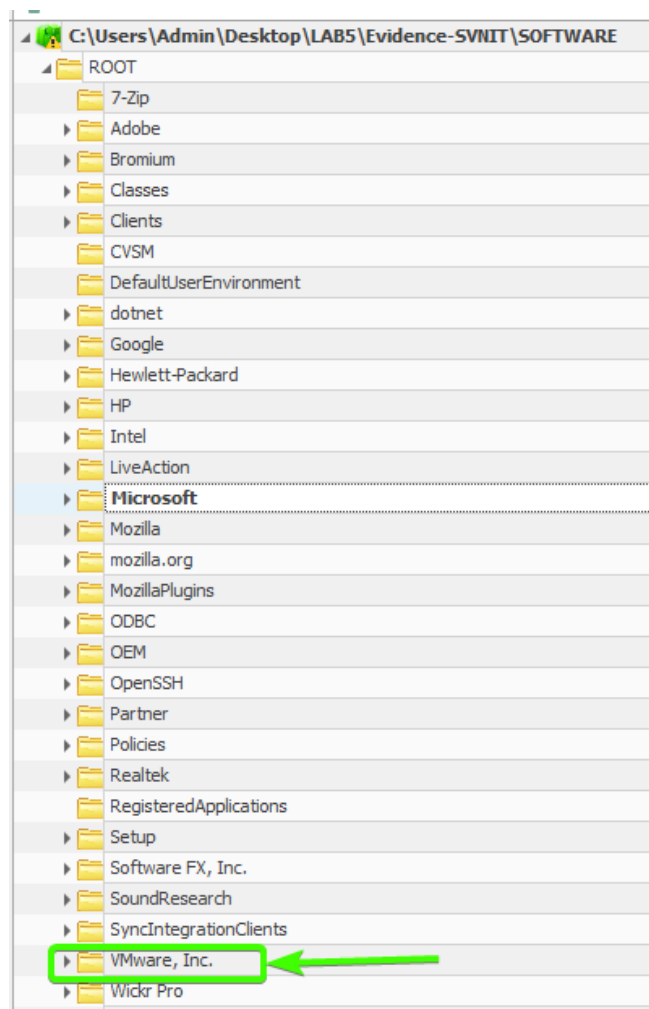
Value Name	Value Type	Data	Value Slack
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealthSystray.exe	00-00-00-00
RtkAudUService	RegSz	"C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_and64_1e9988599ad...	D7-B4-60-05
AdobeGCInvoker-1.0	RegSz	"C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInvokerUtility.exe"	65-72-2E-45

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