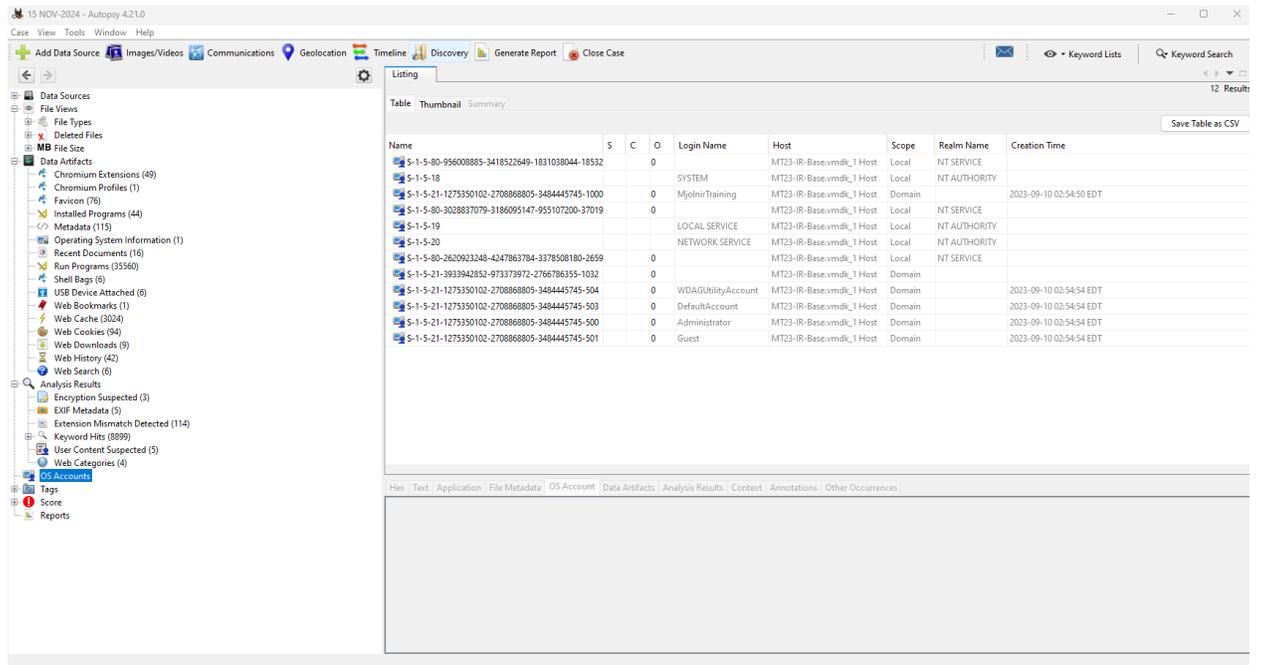


DIGITAL FORENSICS&INCID. RESP - COMP 4071

HOMEWORK LAB 4

1. When was the OS built?



The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, with 'OS Accounts' selected. The main window shows a table listing the accounts. The table has columns for Name, S, C, O, Login Name, Host, Scope, Realm Name, and Creation Time. The table contains 12 rows of data, including accounts like SYSTEM, MjolnirTraining, LOCAL SERVICE, NETWORK SERVICE, and various domain accounts like WDAGUtilityAccount, DefaultAccount, Administrator, and Guest.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-S-80-95600885-3418522649-1831038044-18532			0		MT23-IR-Base.vmdk_1 Host	Local	NT SERVICE	
S-1-S-18				SYSTEM	MT23-IR-Base.vmdk_1 Host	Local	NT AUTHORITY	
S-1-S-21-1275350102-270868805-3484445745-1000			0	MjolnirTraining	MT23-IR-Base.vmdk_1 Host	Domain		2023-09-10 02:54:50 EDT
S-1-S-80-3028837079-3186095147-955107200-37019			0		MT23-IR-Base.vmdk_1 Host	Local	NT SERVICE	
S-1-S-19				LOCAL SERVICE	MT23-IR-Base.vmdk_1 Host	Local	NT AUTHORITY	
S-1-S-20				NETWORK SERVICE	MT23-IR-Base.vmdk_1 Host	Local	NT AUTHORITY	
S-1-S-80-2620923248-4247863784-3378508180-2659			0		MT23-IR-Base.vmdk_1 Host	Local	NT SERVICE	
S-1-S-21-3933942852-973373972-2766786355-1032			0		MT23-IR-Base.vmdk_1 Host	Domain		
S-1-S-21-1275350102-270868805-3484445745-504			0	WDAGUtilityAccount	MT23-IR-Base.vmdk_1 Host	Domain		2023-09-10 02:54:54 EDT
S-1-S-21-1275350102-270868805-3484445745-503			0	DefaultAccount	MT23-IR-Base.vmdk_1 Host	Domain		2023-09-10 02:54:54 EDT
S-1-S-21-1275350102-270868805-3484445745-500			0	Administrator	MT23-IR-Base.vmdk_1 Host	Domain		2023-09-10 02:54:54 EDT
S-1-S-21-1275350102-270868805-3484445745-501			0	Guest	MT23-IR-Base.vmdk_1 Host	Domain		2023-09-10 02:54:54 EDT

10/09/2023

2. Who are the admin users?

Listing | Keyword search 1 - admin | Keyword search 2 - admin | 12 Results

Table | Thumbnail | Summary

Page: Pages: Go to Page: Save Table as CSV

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-18532			0		MT23-IR-...	Local	NT SERVICE	
S-1-5-18				SYSTEM	MT23-IR-...	Local	NT AUTHORITY	
S-1-5-21-1275350102-2708868805-3484445745-1000			0	MjolinrTraining	MT23-IR-...	Domain		2023-09-10 02:54:50 EDT
S-1-5-80-3028837079-3186095147-955107200-37019			0		MT23-IR-...	Local	NT SERVICE	
S-1-5-19				LOCAL SERVICE	MT23-IR-...	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	MT23-IR-...	Local	NT AUTHORITY	
S-1-5-80-2620923248-4247863784-3378508180-2659			0		MT23-IR-...	Local	NT SERVICE	
S-1-5-21-3933942852-973373972-2766786355-1032			0		MT23-IR-...	Domain		
S-1-5-21-1275350102-2708868805-3484445745-504			0	WDAGUtilityAccount	MT23-IR-...	Domain		2023-09-10 02:54:54 EDT
S-1-5-21-1275350102-2708868805-3484445745-503			0	DefaultAccount	MT23-IR-...	Domain		2023-09-10 02:54:54 EDT
S-1-5-21-1275350102-2708868805-3484445745-500			0	Administrator	MT23-IR-...	Domain		2023-09-10 02:54:54 EDT
S-1-5-21-1275350102-2708868805-3484445745-501			0	Guest	MT23-IR-...	Domain		2023-09-10 02:54:54 EDT

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Basic Properties

Login: Administrator
 Full Name:
 Address: S-1-5-21-1275350102-2708868805-3484445745-500
 Type:
 Creation Date: 2023-09-10 02:54:54 EDT
 Object ID: 1228651

MT23-IR-Base.vmdk_226842 Host Details

Login Count: 0
 Description: Built-in account for administering the computer/domain

3. What profile preferences can you find for the users? Name the file and preferences.

GBC - Jan 2024 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing | Keyword Lists | Keyword Search | 34 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Size	Modified Time	Change Time	Access Time	Created Time	Flags(Dir)	Flags(MA)
UNESURVE				136	2023-09-10 02:57:04 EDT	2023-09-10 02:57:04 EDT	2023-09-10 02:57:04 EDT	2023-09-10 02:57:04 EDT	Allocated	Allocate
Pictures				576	2023-09-10 02:57:17 EDT	2023-09-10 02:57:17 EDT	2023-09-21 14:44:29 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
PrintHood				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Recent				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Recent				132	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Saved Games				56	2023-09-10 02:57:13 EDT	2023-09-10 02:57:13 EDT	2023-09-10 02:57:16 EDT	2023-09-10 02:55:02 EDT	Allocated	Allocate
Searches				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
SendTo				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Start Menu				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Templates				48	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
Videos				236	2023-09-12 17:33:36 EDT	2023-09-12 17:33:36 EDT	2023-10-06 18:52:39 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
NTUSER.DAT			0	1310720	2023-09-17 20:01:04 EDT	2023-09-10 02:54:58 EDT	2023-09-17 20:01:04 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
ntuser.dat.LOG1			0	196608	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate
ntuser.dat.LOG2			0	729088	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	2023-09-10 02:54:58 EDT	Allocated	Allocate

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Extracted Text | Translation

Page 1 of 12 Page Matches on page - of - Match 100% Reset Text Source: File Text

```
regf::sems\MjolinrTraining\ntuser.dat
s-mmm
Ofrg
hbin
#ROOT
AppEvents
Shell
pkj
Console
Group1
Group2
Control Panel
UShowCount
S-1-5-32-545
Group4
S-1-5-32-544
```


5. Name the files over 1GB in size and their locations

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, with 'MB 1GB+' selected under 'MB File Size'. The main window shows a table of files over 1GB in size.

Name	S	C	O	Size	Modified Time	Change Time	Access Time	Created Time
pagefile.sys				134217220	2023-09-17 20:01:19 EDT	2023-09-17 20:01:19 EDT	2023-09-17 20:01:19 EDT	2023-09-09
{6ed365b7-5719-11ee-a815-000c29cc0445}{3808876b-c176-4e48-b7ee-04046eccc752}				147449888	2023-09-29 22:01:45 EDT	2023-09-29 22:01:45 EDT	2023-09-29 22:01:45 EDT	2023-09-29
{c747deb3-5ebb-11ee-a815-000c29cc0445}{3808876b-c176-4e48-b7ee-04046eccc752}				181193928	2023-10-07 09:14:09 EDT	2023-10-07 09:14:09 EDT	2023-10-07 09:14:09 EDT	2023-09-29
SW_DVDS_Office_Professional_Plus_2019_32_BIT_X64_English_C2R_X21-84626.ISO				354937612	2021-12-27 11:04:45 EST	2023-09-17 20:19:22 EDT	2023-09-10 03:25:44 EDT	2023-01-06
SW_DVDS_Office_Professional_Plus_2019_32_BIT_X64_English_C2R_X21-84626.ISO				354937612	2021-12-27 11:04:45 EST	2023-09-12 21:57:29 EDT	2023-09-10 03:25:44 EDT	2023-09-10
\$BsdClus\$Bad				160715239424	2023-09-09 22:51:31 EDT	2023-09-09 22:51:31 EDT	2023-09-09 22:51:31 EDT	2023-09-09

The bottom pane shows the 'Strings' view for the selected file, displaying extracted text including 'CD001', '16.0.10730.20102', 'MICROSOFT CORPORATION', and 'CDIMAGE 2.56 (01/01/2005 TM)'.

6. Device ID of virtual mouse

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, with 'USB Device Attached (0)' selected under 'Data Artifacts'. The main window shows a table of USB Device Attached items.

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM				2023-09-17 20:01:19 EDT	ROOT_HUB	58239198b0	MT23-IR-Base.vmdk	
SYSTEM				2023-09-17 20:01:19 EDT	ROOT_HUB20	5836ab54f60	MT23-IR-Base.vmdk	
SYSTEM				2023-09-17 20:01:19 EDT	ROOT_HUB30	5821ab4fc8080	MT23-IR-Base.vmdk	
SYSTEM				2023-09-17 20:01:19 EDT	Virtual Mouse	6630c5d09c&0&5	MT23-IR-Base.vmdk	
SYSTEM				2023-09-17 20:01:19 EDT	Virtual Mouse	783aa299608080001	MT23-IR-Base.vmdk	
SYSTEM				2023-09-17 20:01:19 EDT	Virtual Mouse	783aa299608080001	MT23-IR-Base.vmdk	

The bottom pane shows the 'Strings' view for the selected file, displaying extracted text including 'Script: Latin - Basic'.

1. 6&30c5d09c&0&5

MOHAMAD ALMASR 101167438

2. 7&3ae26960&0&0000

3. 7&3ae26960&0&0001

SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	6830c5d09c&0&0&5	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	783ae26960&0&0&0000	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	783ae26960&0&0&0001	MT23-IR-Base.vmdk

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 4 of 6									USB Device Attached
Type	Value								Source(s)
Date/Time	2023-09-17 20:01:19 EDT								Recent Activity
Device Make	VMware, Inc.								Recent Activity
Device Model	Virtual Mouse								Recent Activity
Device ID	6830c5d09c&0&0&5								Recent Activity
Source File Path	/img_MT23-IR-Base.vmdk/vol_vol6/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854768762								

SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	783ae26960&0&0&0000	MT23-IR-Base.vmdk
SYSTEM	0	2023-09-17 20:01:19 EDT	VMware, Inc.	Virtual Mouse	783ae26960&0&0&0001	MT23-IR-Base.vmdk

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 5 of 6									USB Device Attached
Type	Value								Source(s)
Date/Time	2023-09-17 20:01:19 EDT								Recent Activity
Device Make	VMware, Inc.								Recent Activity
Device Model	Virtual Mouse								Recent Activity
Device ID	783ae26960&0&0&0000								Recent Activity
Source File Path	/img_MT23-IR-Base.vmdk/vol_vol6/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854768761								

Analysis Results

- Encryption Detected (2)
- Encryption Suspected (3)
- EXIF Metadata (5)
- Extension Mismatch Detected (114)
- Keyword Hits (36258)
 - Single Literal Keyword Search (20377)
 - admin (15608)
 - consent (821)**
 - sam (3948)
 - Single Regular Expression Search (0)
 - Email Addresses (15881)
 - User Content Suspected (5)
 - Web Categories (4)
- OS Accounts
- Tags

Listing: Keyword search 3 - consent X

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time	Change Time
megascas.inf			0	the specific written «consent» of LSI Corp., Inc.	consent	2019-12-07 04:07:53 EST	2023-10-07 03:03:16 EDT	2023-09-09 22:51:55 E
Unaloc_1_0_1073741824			0	successfully updated the «consent» status on server si...	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Unaloc_1_2147483648_321225472			0	extension/policies"/>«consent»mgbehavioradmi...	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Unaloc_1_1073741824_2147483648			0	se-AppContainer-Skip-«Consent»-DialogDPI-AppDat...	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f1947664.txt			0] "application/edi-«consent»: ["source": "ima	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ProtectionManagement.mnfl			0	ng: [Description]"«Consent» for sample submission	consent	2019-12-07 09:44:18 EST	2019-12-07 09:44:18 EST	2023-09-09 22:51:41 E
Mp4aDesc.dll.mui			0	nts without adequate «consent».A program that collect	consent	2021-04-09 09:45:33 EDT	2023-09-11 03:06:58 EDT	2023-09-10 09:48:51 E
f0974776.dll			0	se-AppContainer-Skip-«Consent»-DialogChangeDesk...	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
pcalua.exe			0	launch application with «consent» [%d]System32\Sys...	consent	2023-09-10 05:51:19 EDT	2023-09-12 17:32:43 EDT	2023-09-12 17:32:40 E
wemgr.exe			0	itionalDataDisabled-Consent-DefaultConsentDefaul	consent	2023-09-10 05:52:51 EDT	2023-09-12 17:32:44 EDT	2023-09-12 17:32:41 E
ac-discovery-27f1312365c0bb4ec873.js			0	file"«%e.CONSENTE?»-«CONSENT»-«eA-PCG_SUGGE...	consent	2023-07-31 13:08:11 EDT	2023-09-11 09:06:25 EDT	2023-09-10 08:39:51 E
Windows.Security.Credentials.UIUserConsentVerif			0	"to needs your «consent»Allow «Consent»-Verification...	consent	2019-12-07 09:44:20 EST	2019-12-07 09:44:20 EST	2023-09-09 22:52:14 E
mig_protection_sdb.dll			0	grant «consent» to access User granted «consent» to a...	consent	2023-09-29 08:16:32 EDT	2023-10-05 22:01:27 EDT	2023-10-02 16:59:12 E
Win32CompatibilityAppraiser_DOF.xml			0	advanced policies, and WER «consent» policies) is call...	consent	2019-12-07 04:08:53 EST	2023-09-11 03:11:52 EDT	2023-09-12 16:59:09 E
enterprises.tsv			0	Navitel s.o.e.48983 Open «Consent»-Group48984 ...	consent	2023-08-23 15:03:38 EDT	2023-09-11 09:07:01 EDT	2023-09-10 03:33:20 E
f0696908.dll			0	virtual smart card delete «consent»-PIN policy(The smart	consent	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
wemgr.exe			0	itionalDataDisabled-Consent-DefaultConsentDefaul	consent	2023-09-12 16:37:50 EDT	2023-09-12 17:32:48 EDT	2023-09-12 17:32:48 E
wer.dll			0	downs>Error Reporting/v-Consent-NewUserDefaultCons...	consent	2023-09-10 05:52:51 EDT	2023-09-24 08:01:54 EDT	2023-09-12 17:32:41 E
DriverVitalManagement.dll.mui			0	Flashba@Bazr&Aucurwul/«consent» for sample submissi...	consent	2016-12-07 09:48:18 EST	2016-12-07 09:48:18 EST	2016-06-06 23:41:41 E