

Lab 1: Imaging and Recovering Files

R. Harini

18BCE1010

1. Using AccessData FTK Imager

Procedure:

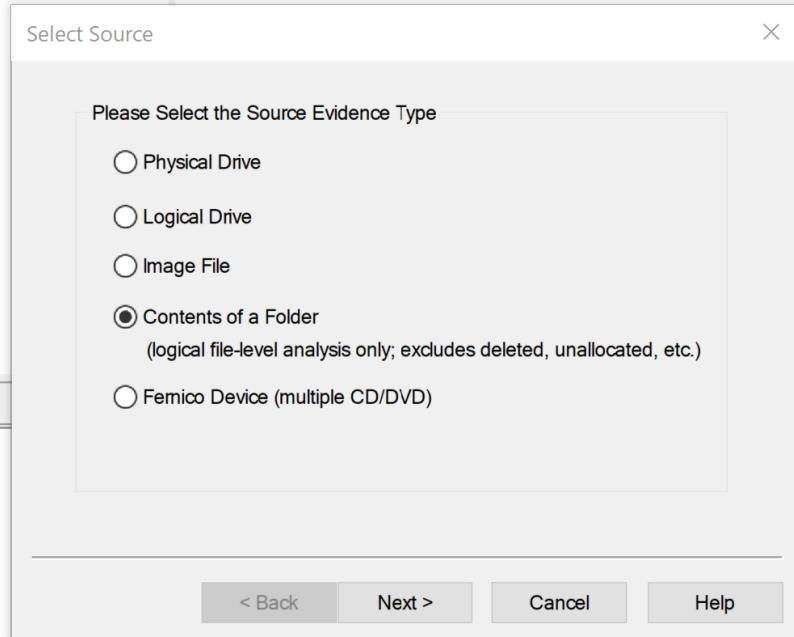
Delete a File from the folder that needs to be recovered later. In this case, delete “Blogging.docx”

Create an image of the folder using FTK Imager

File -> Create Disk Image -> Select Source -> Contents of a Folder -> Enter Image Source Path of the Folder -> Add in Image Destination -> Enter Image Destination Folder and File Name -> Finish -> Start

Using RecoverMyFiles, recover deleted file from the Image

Screenshots:



Select File X

Evidence Source Selection

Please enter the source path:

C:\Users\rhari\Desktop\Harini\Enactus

Create Image X

Image Source

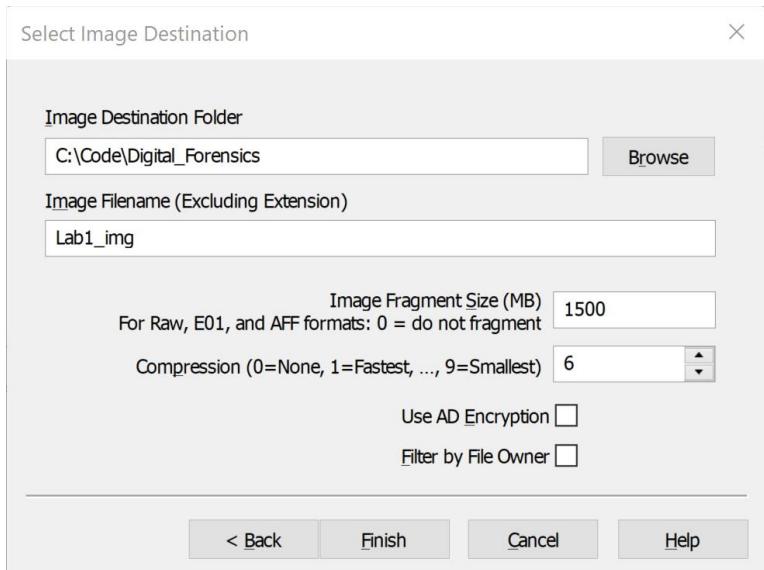
C:\Users\rhari\Desktop\Harini\Enactus

Starting Evidence Number:

Image Destination(s)

Verify images after they are created Precalculate Progress Statistics

Create directory listings of all files in the image after they are created



Drive/Image Verify Results	
<input type="checkbox"/>	
Name	Lab1_img.ad1
MD5 Hash	
Computed hash	42176be7922611c261e5b9aa1e8ced28
Report Hash	42176be7922611c261e5b9aa1e8ced28
Verify result	Match
SHA1 Hash	
Computed hash	82fdd31563359c7e870e664875d2d19ec243
Report Hash	82fdd31563359c7e870e664875d2d19ec243
Verify result	Match
<input type="button" value="Close"/>	

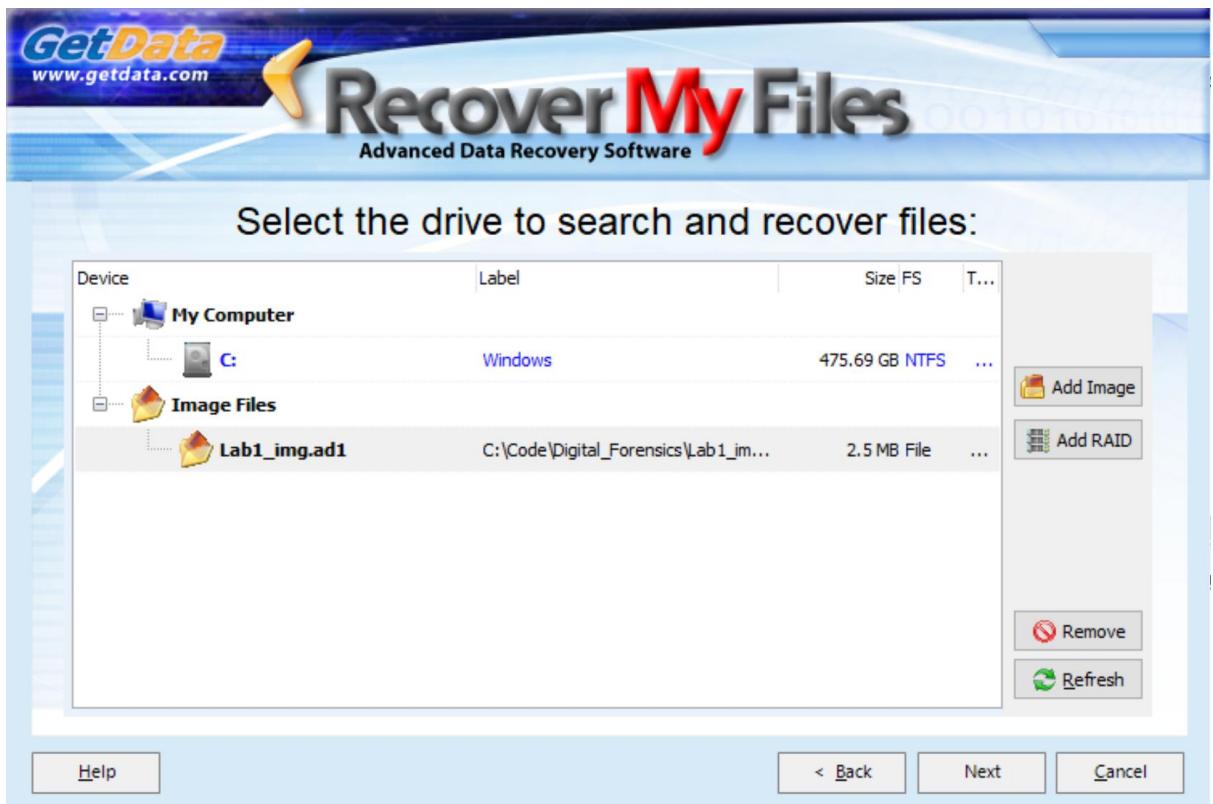
2. Using RecoverMyFiles tool

Procedure:

Recover Files -> Add Image -> Select the Image file created earlier -> Press Next

Under File List, you can view all the files inside the folder that were deleted.

Outputs:



RecoverMyFiles										
RecoverMyFiles v6.3.2(2552) (64-bit) [Evaluation]										
Start Recovery Save Session Load Session Validate Options Deleted Files: 0 Search Completed Skip Update About Help Buy Activate										
Folders File Type Deleted Date File List Gallery View										Search Progress
1	Banana Leaves As Packaging.docx	docx	278,677	3/5/2020 4:55:49 PM	3/1/2020 2:16:09 PM	3/5/2020 4:55:49				
2	Blogging.docx	docx	15,967	4/14/2020 8:01:46 AM	4/13/2020 7:16:22 PM	4/14/2020 8:01:				
3	Coco_Project.docx	docx	11,786	4/6/2020 2:16:53 PM	4/6/2020 2:16:52 PM	4/6/2020 2:16:5				
4	M&S.docx	docx	12,358	3/27/2020 3:02:26 PM	3/27/2020 2:26:07 PM	3/27/2020 3:02:				
5	M&S_Questions.docx	docx	14,319	14,319	4/1/2020 6:44:23 AM	4/1/2020 6:44:22 AM	4/1/2020 6:44:2			
6	Maler - Ideas for Incense.docx	docx	340,681	340,681	2/8/2021 6:33:12 AM	2/8/2021 5:45:46 AM	2/8/2021 6:33:1			
7	Maler .docx	docx	15,168	15,168	10/27/2020 6:29:55 AM	10/27/2020 6:29:54 AM	10/27/2020 6:29			
8	Questions.docx	docx	14,262	14,262	4/1/2020 6:44:02 AM	4/1/2020 6:44:01 AM	4/1/2020 6:44:0			
9	Resin accessories.docx	docx	1,916,585	1,916,585	11/19/2020 2:01:13 PM	11/19/2020 1:21:30 PM	11/19/2020 2:01			
10	Toda Art Form.docx	docx	15,329	15,329	4/10/2020 6:09:50 AM	4/9/2020 6:12:58 PM	4/10/2020 6:09:			
11	Ujjwal.docx	docx	12,966	12,966	4/2/2020 11:49:10 AM	4/2/2020 11:49:10 AM	4/2/2020 11:49:			
12	Wari Art.docx	docx	11,942	11,942	3/27/2020 7:00:27 AM	3/27/2020 7:00:27 AM	3/27/2020 7:00:			
13	Writeup.docx	docx	14,701	14,701	10/13/2019 1:58:56 PM	10/11/2019 2:59:23 PM	10/13/2019 1:58			

Lab 2: Integrity Checking

R. Harini

18BCE1010

Aim: To check the integrity of the files with the help of Hash Values

Procedure: Upload the File onto the website [MD5 File - HTML5 File Hash Online Calculator - MD5, SHA1, SHA2 \(SHA-256\), SHA-384, SHA-512](#) and calculate the Hash Values

Outputs:

1. Original PowerPoint

Hash functions.pptx	(n/a) - 279933 bytes
MD5	244ed853d227771b38fe786015b803e9
SHA-1	84e4ff174c5737f347b729461bbccde3fc756
SHA-256	e6b393ccb8869fa8fe84993ef44c155872c47437e213b7bbba2ad55495ec81
SHA-384	c1b37595ac61ce9c703f507aada1e9367ecade9c47997270bfc71aaa3a0269cade25d9eb4de98b01240271411d3cd109
SHA-512	3875413128696d0cae644659983baaccb744603fdcc29d6a3f0adc78ca1325a218c7c27d12e672d886575e105350c6e04b9fe93778ecd9364291d851edc064

MD5: 244ed853d227771b38fe786015b803e

Modified PowerPoint

Hash functions.pptx	(n/a) - 280176 bytes
MD5	1a81781daaa079f414458c5081eebfbf
SHA-1	07cd2e54633b454c45007e729ed53cebd6ff78c
SHA-256	ff580c6728204790ab07e6c88bd040b56e0951e450d1058ff504786b9f842ca0
SHA-384	060fb8823e1c2989e385427f1657106b76776e7da838a782c467236db335695c5150161734d59790023a77732acd4972
SHA-512	469757646d6555ab2bdcce18bd3d1353263072111f3d6f1104b59957c6b95904d3aed877c166ba82278adff9c88548e4021efbcf7dd1cf1c1bef38399a8

MD5: 1a81781daaa079f414458c5081eebfbf

Since there is A **CHANGE** in the Hash value, we can infer that the file has been modified.

2. Original Image

joey-kyber-Pihl8kTtx-s-unsplash.jpg	(image/jpeg) - 3924249 bytes
MD5	5fd42972609085d2441f47bf191220d5
SHA-1	8fc6190d5050635713748ffd41e4acac05f6a86f
SHA-256	db14e99afdc5d93baacd180ec3e01d0e402d284cb3275d1d06b824e3a5de48ab
SHA-384	184da9fa794dbd14b7f354f7f53106c44de40be0773ff05376b87d8e444fb2e5e08a3a69e45a20d2ad265a11c9ff4d
SHA-512	96f45a2117a606d7e013c775a62920c0b610d1a680b726e80a4472b7683a54eebeab73fb87fea4ef5e351fe211e69fd7c79dadbe910e738ee2154acde528cb7

MD5: 5fd42972609085d2441f47bf191220d5

Un-modified Image

joey-kyber-Pihl8kTtx-s-unsplash.jpg	(image/jpeg) - 3924249 bytes
MD5	5fd42972609085d2441f47bf191220d5
SHA-1	8fc6190d5050635713748ffd41e4acac05f6a86f
SHA-256	db14e99afdc5d93baacd180ec3e01d0e402d284cb3275d1d06b824e3a5de48ab
SHA-384	184da9fa794dbd14b7f354f7f53106c44de40be0773ff05376b87d8e444fb2e5e08a3a69e45a20d2ad265a11c9ff4d
SHA-512	96f45a2117a606d7e013c775a62920c0b610d1a680b726e80a4472b7683a54eebeab73fb87fea4ef5e351fe211e69fd7c79dadbe910e738ee2154acde528cb7

MD5: 5fd42972609085d2441f47bf191220d5

Since there is **NO CHANGE** in the Hash values, we can infer that the file has not been modified.

Lab 3: File Analysis Tools

R. Harini

18BCE1010

Algorithm / Procedure: Download and install Microsoft's Log Parser tool for the Windows environment from Microsoft's Web Site.

<https://www.microsoft.com/en-in/download/details.aspx?id=24659>

Tutorial Link: [Log Parser Tutorial: Learn to Parse Many Input Formats | Scalyr](#)

Output:

- 1) LogParser "SELECT LogFileName as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT LogFileName as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
-----
C:\Windows\Logs\CMS\CMS.log
Press a key...
Task aborted by user.

Statistics:
-----
Elements processed: 31
Elements output:    30
Execution time:     2.59 seconds
```

- 2) LogParser "SELECT Index as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Index as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
-----
1
2
3
4
5
6
7
8
9
10
Press a key...
Task aborted by user.

Statistics:
-----
Elements processed: 31
Elements output:    30
Execution time:     1.56 seconds
```

3) LogParser "SELECT Text as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Text as LineFromFile FROM C:\Windows\Logs\CMS\CMS.log
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
-----
2021-02-14 19:10:15, Info          CBS      TI: --- Initializing Trusted Installer ---
2021-02-14 19:10:15, Info          CBS      TI: Last boot time: 2021-02-14 19:09:58.500
2021-02-14 19:10:15, Info          CBS      Starting TrustedInstaller initialization.
2021-02-14 19:10:15, Info          CBS      Lock: New lock added: CCbsPublicSessionClassFactory, level:
30, total lock:4
2021-02-14 19:10:15, Info          CBS      Lock: New lock added: CCbsPublicSessionClassFactory, level:
30, total lock:5
2021-02-14 19:10:15, Info          CBS      Lock: New lock added: WinlogonNotifyLock, level: 8, total lo
ck:6
2021-02-14 19:10:15, Info          CBS      Ending TrustedInstaller initialization.
2021-02-14 19:10:15, Info          CBS      Starting the TrustedInstaller main loop.
2021-02-14 19:10:15, Info          CBS      TrustedInstaller service starts successfully.
2021-02-14 19:10:15, Info          CBS      Winlogon: Registering for CreateSession notifications
Press a key...
Task aborted by user.

Statistics:
-----
Elements processed: 31
Elements output:    30
Execution time:     2.63 seconds
```

Lab 4: Event Viewer and Event Log Explorer Tool

R. Harini

18BCE1010

Procedure: Open Event Viewer tool that is inbuilt in the Windows OS

Windows Log -> Security

Click on any one Event to view its properties and Details

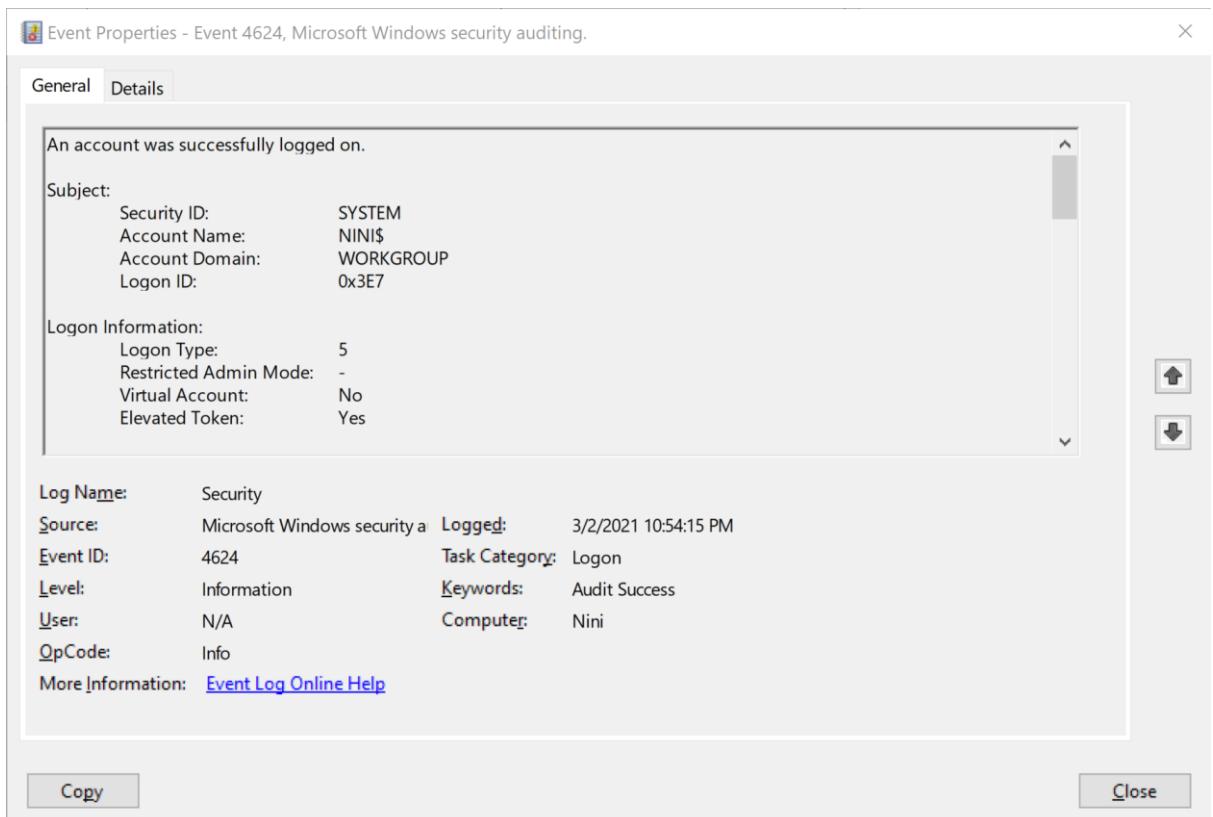
Event Viewer

a) Successful Logon

The screenshot shows the 'Event Properties' dialog box for Event 4624. The title bar reads 'Event Properties - Event 4624, Microsoft Windows security auditing.' The 'General' tab is selected. Below it, there are two radio buttons: 'Friendly View' (selected) and 'XML View'. The main pane displays event details under the 'System' category, with the 'EventData' section expanded. The data includes:

- SubjectUserId**: S-1-5-18
- SubjectUserName**: NINI\$
- SubjectDomainName**: WORKGROUP
- SubjectLogonId**: 0x3e7
- TargetUserId**: S-1-5-18
- TargetUserName**: SYSTEM
- TargetDomainName**: NT AUTHORITY
- TargetLogonId**: 0x3e7
- LogonType**: 5
- LogonProcessName**: Advapi
- AuthenticationPackageName**: Negotiate
- WorkstationName**: -
- LogonGuid**: {00000000-0000-0000-0000-000000000000}

On the right side of the dialog, there are vertical scroll bars and three small control buttons: an up arrow, a down arrow, and a double arrow.



b) Failed logon

Event Viewer

File **Action** **View** **Help**

Security Number of events: 35,041 (0 New events available)

Keywords Date and Time Source Event ID Task Category

Audit Failure	3/4/2021 20:05 PM	Microsoft Windows security	5061	System
Audit Failure	3/4/2021 20:05 PM	Microsoft Windows security	5061	System
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:04 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.
Audit Success	3/4/2021 20:03 PM	Microsoft Windows security	5379	User Ac.

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 5061, Microsoft Windows security auditing.

General **Details**

Cryptographic operation.

Subject:

Security ID:	NINI\$\\rhari
Account Name:	rhari
Account Domain:	Nini
Logon ID:	0xD4978

Log Name: Security
Source: Microsoft Windows security
Event ID: 5061
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Event Properties - Event 5061, Microsoft Windows security auditing.

General Details

Friendly View XML View

+ System
- EventData

SubjectUserId S-1-5-21-2298830179-1136938727-1749915843-1001
SubjectUserName rhari
SubjectDomainName NINI
SubjectLogonId 0xda978
ProviderName Microsoft Software Key Storage Provider
AlgorithmName UNKNOWN
KeyName TB_0_office.com
KeyType %%2500
Operation %%2480
ReturnCode 0x80090016

Copy **Close**

Event Properties - Event 5061, Microsoft Windows security auditing.

General Details

Cryptographic operation.

Subject:
 Security ID: NINI\rhari
 Account Name: rhari
 Account Domain: NINI
 Logon ID: 0xDA978

Cryptographic Parameters:
 Provider Name: Microsoft Software Key Storage Provider
 Algorithm Name: UNKNOWN
 Key Name: TB_0_office.com
 Key Type: User key.

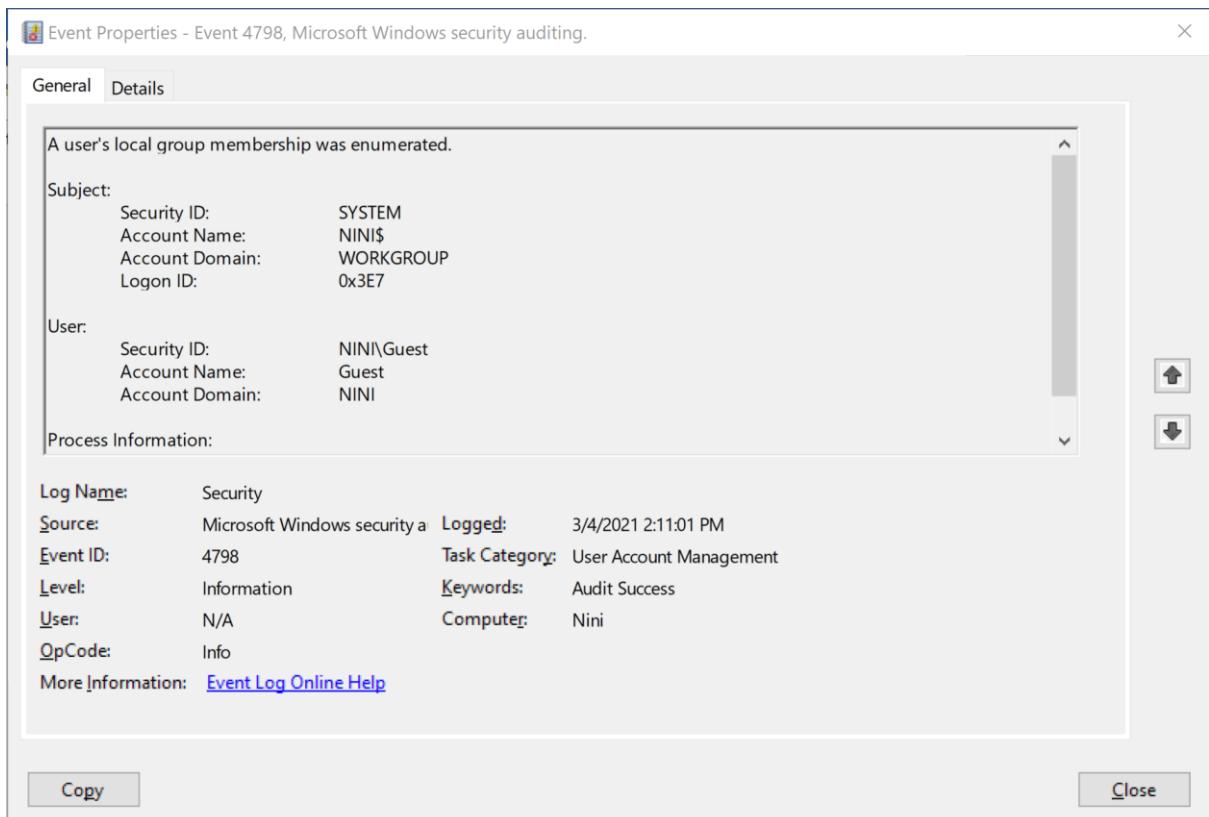
Log Name: Security
Source: Microsoft Windows security a Logged: 3/4/2021 2:09:05 PM
Event ID: 5061 Task Category: System Integrity
Level: Information Keywords: Audit Failure
User: N/A Computer: Nini
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

c) A new user was created

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Security selected), Setup, System, Forwarded Events, Applications and Services Log, and Subscriptions. The right pane shows the Security log with 35,041 events. A detailed view of event 4798 is open, titled "Event 4798, Microsoft Windows security auditing". The event details show it was logged at 3/4/2021 2:11:01 PM by User Ac.. The subject was SYSTEM, and the logon ID was 0x3e7. The event category is User Account Management, and the task category is User Account Management. The event type is Information, and the user was N/A. The OpCode was Info. The event data indicates a user's local group membership was enumerated.

The screenshot shows the "Event Properties - Event 4798, Microsoft Windows security auditing" dialog. The General tab is selected, showing the event details: TargetUserName Guest, TargetDomainName NINI, TargetSid S-1-5-21-2298830179-1136938727-1749915843-501, SubjectUserId S-1-5-18, SubjectUserName NINI\$, SubjectDomainName WORKGROUP, SubjectLogonId 0x3e7, CallerProcessId 0x8f4, and CallerProcessName C:\Windows\System32\svchost.exe. Below these details are two buttons: "Copy" and "Close".



Event Log Explorer Tool

- a) Successful Logon

Security on NINI							
	Type	Date	Time	Event	Source	Category	User
Application (29436)	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Hardware Events (0)	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Initial Logon (0)	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Intel-GFX-InfoApp	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Intel-GFX-InfoSyst	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Internet Explorer (0)	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Key Management (0)	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Leverage-Power	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Lenovo-Sf-Compan	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Lenovo-Sf-CorpQ	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Lenovo-Sf-Device	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Lenovo-Sf-Setting	ForwardedEvents	3/4/2021	2:22:38 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Appl-Cle	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Appl-Cle	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Client-Usa	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Elc-Usa	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Group-Confir	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Itsl-Logon	ForwardedEvents	3/4/2021	2:20:59 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-User-Exp	ForwardedEvents	3/4/2021	2:19:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-User-Exp	ForwardedEvents	3/4/2021	2:19:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-User-Exp	ForwardedEvents	3/4/2021	2:19:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Microsoft-Windows	ForwardedEvents	3/4/2021	2:19:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Network Isolation (0)	ForwardedEvents	3/4/2021	2:19:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
OpenSSH/Admin (0)	ForwardedEvents	3/4/2021	2:18:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
OpenSSH/Operator	ForwardedEvents	3/4/2021	2:18:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
RemoteDesktopSer	ForwardedEvents	3/4/2021	2:18:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
RemoteDesktopSer	ForwardedEvents	3/4/2021	2:18:40 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Security (35040)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Setup (268)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
SGU-User (918)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
SMsApp (42)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
SMsApp (0)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
System (38166)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Windows Azure (0)	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Windows Networkin	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Windows Networkin	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
Windows Power She	ForwardedEvents	3/4/2021	2:17:50 PM	0x8000000000000000	Microsoft-Windows-Security-Access	Audit Success	Nini
A user's local group membership was enumerated.							
Subject:	Security ID:	S-1-5-18					
	Account Name:	NINIS					
	Account Domain:	WORKGROUP					
	Logon ID:	0000003E7					
User:	Security ID:	S-1-5-21-2298830179-1136938727-1749915943-1001					
	Account Name:	rhan					
	Account Domain:	NINE					
Process Information:	Process ID:	000000BF4					
	Description:	Windows PowerShell					

b) Failed logon

Type	Date	Time	Event	Source	Category	User	Computer
Audit Failure	3/4/2021	2:09:05 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/4/2021	2:09:05 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/4/2021	2:09:03 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	4:31:57 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	4:31:55 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	2:09:03 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	10:00:18 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	10:00:16 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/3/2021	10:00:16 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	10:54:07 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	10:54:06 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	10:54:05 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	9:19:39 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	9:19:19 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	9:19:19 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	5:00:28 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	5:00:26 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	5:00:25 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	3:44:43 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	3:44:41 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	3:44:41 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	11:28:14 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	11:28:13 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/2/2021	11:28:11 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	5:40:08 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	5:40:06 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	5:40:04 PM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	8:08:49 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	8:08:48 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	
Audit Failure	3/1/2021	8:08:48 AM	5061	Microsoft-Windows-SeSystem Integrity	N/A	Nini	

Event Properties - Security on NINI

Standard XML

Date:	3/3/2021	Source:	Microsoft-Windows-Security-Auditing										
Time:	4:31:55 PM	Category:	System Integrity										
Type:	Audit Failure	Event ID:	5061										
User:	N/A												
Computer:	Nini												
Description:	<p>Cryptographic operation.</p> <p>Subject:</p> <table border="1"> <tbody> <tr> <td>Security ID:</td> <td>S-1-5-21-2298830179-1136938727-1749915843-</td> </tr> <tr> <td>1001</td> <td></td> </tr> <tr> <td>Account Name:</td> <td>rhari</td> </tr> <tr> <td>Account Domain:</td> <td>NINI</td> </tr> <tr> <td>Logon ID:</td> <td>000DA978</td> </tr> </tbody> </table>			Security ID:	S-1-5-21-2298830179-1136938727-1749915843-	1001		Account Name:	rhari	Account Domain:	NINI	Logon ID:	000DA978
Security ID:	S-1-5-21-2298830179-1136938727-1749915843-												
1001													
Account Name:	rhari												
Account Domain:	NINI												
Logon ID:	000DA978												
Data:	<input checked="" type="radio"/> Bytes	<input type="radio"/> Words	<input type="radio"/> D-words										
Lookup in:	Event ID Database	Microsoft Knowledge base	Close										

Lab 5: Encoding and Decoding using DCode

R. Harini

18BCE1010

1) Using DCode Tool

The screenshot shows the DCode v5.2 application window. The menu bar includes File, Tools, Theme, and Help. The toolbar has Time Decoding and Time Encoding buttons, with Time Encoding selected. The main area contains a table of time formats and their corresponding values. On the right, there are three panels: Date Input (Pattern: yyyy-'MM'-dd HH:mm:ss'.fff, Value: 2021-03-24 18:24:19.650, Encode button), Time Zone (Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi, No Adjustment, Select buttons), and Value Output (Format: Numeric).

Name	Value
123 Absolute Time (Double)	638283259.65
123 Absolute Time (ns) (Int64)	638283259650000000
123 Apple HFS (Int64)	3699455060
123 Apple HFS+ (Int64)	3699435260
123 Google Chrome (Int64)	13261064059650000
123 GPS Time (Int32)	1300625660
123 Microsoft Ticks (Int64)	5249207891023887904
123 Nokia Series 30 (Int32)	-908017540
123 OLE Automation (Double)	44279.5377274306
123 Unix Seconds (Int32)	1616590460
123 Unix Milliseconds (Java Time) (Int64)	1616590459650
123 Unix Microseconds (Int64)	1616590459650000
123 Windows Filetime (Int64)	132610640596500000

The screenshot shows the DCode v5.2 application window with the Time Decoding tab selected. The main area contains a table of timestamp formats and their corresponding values. On the right, there are three panels: Value Input (Format: Hexadecimal (Little-Endian), Value: 1234, Decode button), Time Zone (Name: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi, No Adjustment, Select buttons), and Date Output (Pattern: yyyy-'MM'-dd HH:mm:ss'.ffffffff K, Sample: 2021-03-24 18:23:57.6281129 +05:30, Default button).

Name	Timestamp
Apple Absolute Time (ns) (UTC)	2001-01-01 00:00:00.0000133 Z
Apple Absolute Time (ns)	2001-01-01 05:30:00.0000133 +05:30
Apple HFS (Local)	1904-01-01 03:42:10.0000000
Apple HFS+ (UTC)	1904-01-01 03:42:10.0000000 Z
Apple HFS+	1904-01-01 09:12:10.0000000 +05:30
Google Chrome (UTC)	1601-01-01 00:00:00.0133300 Z
Google Chrome	1601-01-01 05:30:00.0133300 +05:30
GPS Time (UTC)	1980-01-06 03:42:10.0000000 Z
GPS Time	1980-01-06 09:12:10.0000000 +05:30
Microsoft Ticks (Local)	0001-01-01 00:00:00.0013300
Nokia Series 30 (UTC)	2050-01-01 03:42:10.0000000 Z
Nokia Series 30	2050-01-01 09:12:10.0000000 +05:30
Unix Seconds (UTC)	1970-01-01 03:42:10.0000000 Z
Unix Seconds	1970-01-01 09:12:10.0000000 +05:30
Unix Milliseconds (Java Time) (UTC)	1970-01-01 00:00:13.3300000 Z
Unix Milliseconds (Java Time)	1970-01-01 05:30:13.3300000 +05:30

2) Using String.exe

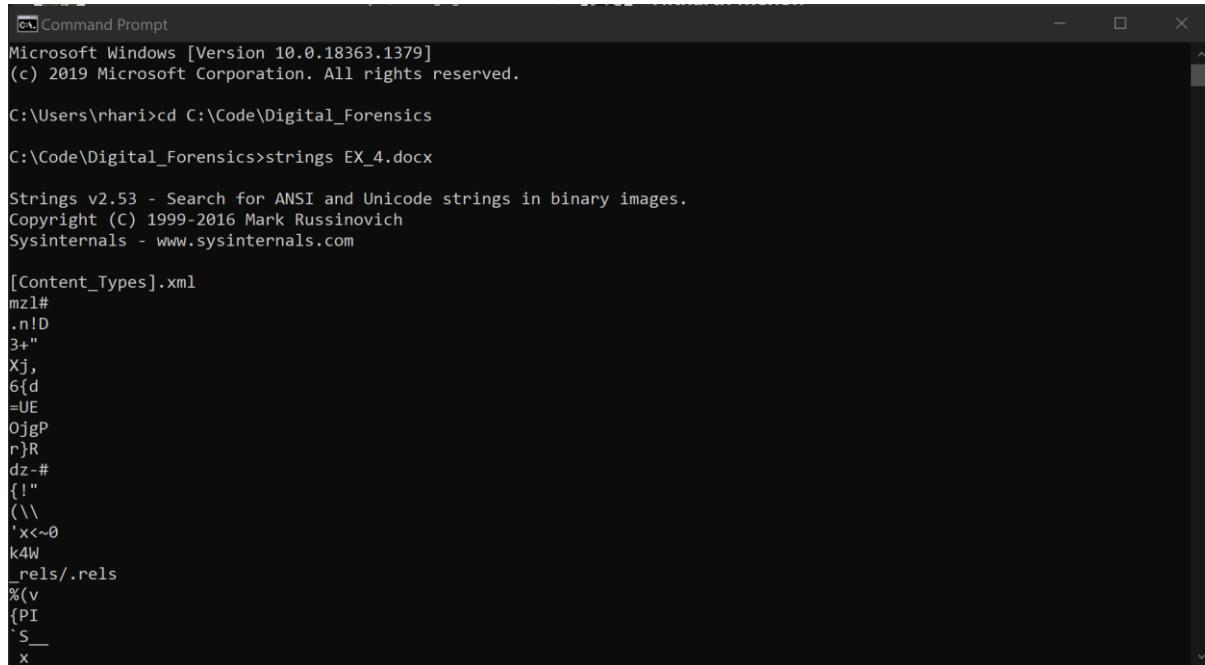
Procedure:

Open cmd

Navigate to the path with the .docx file

Type **strings <filename>.docx**

Output:



```
Command Prompt
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\rhari>cd C:\Code\Digital_Forensics

C:\Code\Digital_Forensics>strings EX_4.docx

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

[Content_Types].xml
mzl#
.n!D
3+
Xj,
6{d
=UE
0jgp
r}R
dz-#
{! "
(\ \
'x<>0
k4W
_rels/.rels
%v
{fI
`S_
_x
```

Lab 6: Using Windows CMD line

R. Harini

18BCE1010

Aim: To become familiar with the Windows command line for digital forensics investigations

1) Use commands to find the IPv4 address and subnet mask of your computer.

Procedure: Using ipconfig command

IPv4: 172.17.136.177

Subnet mask: 255.255.255.240

```

Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\rhari>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::38e6:47d7:b615:7aba%14
    IPv4 Address. . . . . : 192.168.1.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::24ae:9ce8:140:6935%21
    IPv4 Address. . . . . : 192.168.246.33
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . :

Ethernet adapter vEthernet (HvsiIcs):

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::f53c:bcf5:6120:5033%55
    IPv4 Address. . . . . : 172.17.136.177
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . :

```

- 2) Create a batch file that will capture the following volatile information from an evidence system and store it in a file.**

Code:

```

@echo off

FOR /F "delims=: tokens=2" %%a in ('ipconfig ^| find "IPv4"') do set _IPAddress=%a

ECHO IP address is: %_IPAddress% >> grv.txt

```

```
For /f "tokens=2-4 delims=/ " %%a in ('date /t') do (set mydate=%c-%a-%b)
```

```
For /f "tokens=1-2 delims=/:" %%a in ('time /t') do (set mytime=%a%%b)
```

```
echo Date: %mydate% >>grv.txt
```

```
echo Time: %mytime% >>grv.txt
```

```
echo. >>grv.txt
```

```
echo ARP Table >>grv.txt
```

```
FOR /L %%A IN (1,1,5) DO (
```

```
arp -a | findstr 20-7c-8f-3f-03-9c
```

```
cls
```

```
if %errorlevel% GEQ 1 (
```

```
echo The device is offline
```

```
Echo Device is offline at %time% on %date%. >> grv.txt
```

```
) else (
```

```
echo The device is online.
```

```
Echo Device is online at %time% on %date%. >> grv.txt
```

```
)
```

```
timeout 3 >nul /nobreak
```

```
)
```

```
echo. >>grv.txt
```

```
echo Network Connection Information >>grv.txt
```

```
netstat -a>>grv.txt
```

Screenshots:

grv.txt - Notepad

File Edit Format View Help

IP address is: 172.17.136.177

Date: 2021-03-18

Time: 0250 PM

ARP Table

Device is online at 14:50:25.57 on Thu 03/18/2021.
Device is online at 14:50:25.57 on Thu 03/18/2021.

Network Connection Information

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:7	Nini:0	LISTENING
TCP	0.0.0.0:9	Nini:0	LISTENING
TCP	0.0.0.0:13	Nini:0	LISTENING
TCP	0.0.0.0:17	Nini:0	LISTENING
TCP	0.0.0.0:19	Nini:0	LISTENING
TCP	0.0.0.0:80	Nini:0	LISTENING
TCP	0.0.0.0:135	Nini:0	LISTENING
TCP	0.0.0.0:445	Nini:0	LISTENING
TCP	0.0.0.0:623	Nini:0	LISTENING
TCP	0.0.0.0:1801	Nini:0	LISTENING
TCP	0.0.0.0:2103	Nini:0	LISTENING
TCP	0.0.0.0:2105	Nini:0	LISTENING
TCP	0.0.0.0:2107	Nini:0	LISTENING
TCP	0.0.0.0:2179	Nini:0	LISTENING
TCP	0.0.0.0:3389	Nini:0	LISTENING
TCP	0.0.0.0:5040	Nini:0	LISTENING
TCP	0.0.0.0:5357	Nini:0	LISTENING
TCP	0.0.0.0:7070	Nini:0	LISTENING
TCP	0.0.0.0:16992	Nini:0	LISTENING
TCP	0.0.0.0:22350	Nini:0	LISTENING
TCP	0.0.0.0:27036	Nini:0	LISTENING
TCP	0.0.0.0:49664	Nini:0	LISTENING
TCP	0.0.0.0:49665	Nini:0	LISTENING
TCP	0.0.0.0:49666	Nini:0	LISTENING
TCP	0.0.0.0:49667	Nini:0	LISTENING
TCP	0.0.0.0:49668	Nini:0	LISTENING
TCP	0.0.0.0:49669	Nini:0	LISTENING
TCP	0.0.0.0:49678	Nini:0	LISTENING
TCP	0.0.0.0:49765	Nini:0	LISTENING
TCP	0.0.0.0:51635	Nini:0	LISTENING
TCP	0.0.0.0:51636	Nini:0	LISTENING
TCP	127.0.0.1:27015	Nini:0	LISTENING
TCP	127.0.0.1:27060	Nini:0	LISTENING
TCP	127.0.0.1:46621	Nini:0	LISTENING

TCP	192.168.246.33:139	Nini:0	LISTENING
TCP	[::]:7	Nini:0	LISTENING
TCP	[::]:9	Nini:0	LISTENING
TCP	[::]:13	Nini:0	LISTENING
TCP	[::]:17	Nini:0	LISTENING
TCP	[::]:19	Nini:0	LISTENING
TCP	[::]:80	Nini:0	LISTENING
TCP	[::]:135	Nini:0	LISTENING
TCP	[::]:445	Nini:0	LISTENING
TCP	[::]:623	Nini:0	LISTENING
TCP	[::]:1801	Nini:0	LISTENING
TCP	[::]:2103	Nini:0	LISTENING
TCP	[::]:2105	Nini:0	LISTENING
TCP	[::]:2107	Nini:0	LISTENING
TCP	[::]:2179	Nini:0	LISTENING
TCP	[::]:3389	Nini:0	LISTENING
TCP	[::]:5357	Nini:0	LISTENING
TCP	[::]:16992	Nini:0	LISTENING
TCP	[::]:22350	Nini:0	LISTENING
TCP	[::]:49664	Nini:0	LISTENING
TCP	[::]:49665	Nini:0	LISTENING
TCP	[::]:49666	Nini:0	LISTENING
TCP	[::]:49667	Nini:0	LISTENING
TCP	[::]:49668	Nini:0	LISTENING
TCP	[::]:49669	Nini:0	LISTENING
TCP	[::]:49678	Nini:0	LISTENING
TCP	[::]:49765	Nini:0	LISTENING
TCP	[::]:51636	Nini:0	LISTENING
TCP	[::1]:49674	Nini:0	LISTENING
UDP	0.0.0.0:7	*:*	
UDP	0.0.0.0:9	*:*	