Lab 1: Imaging and Recovering Files

R. Harini

18BCE1010

1. Using AccessData FTK Imager

Procedure:

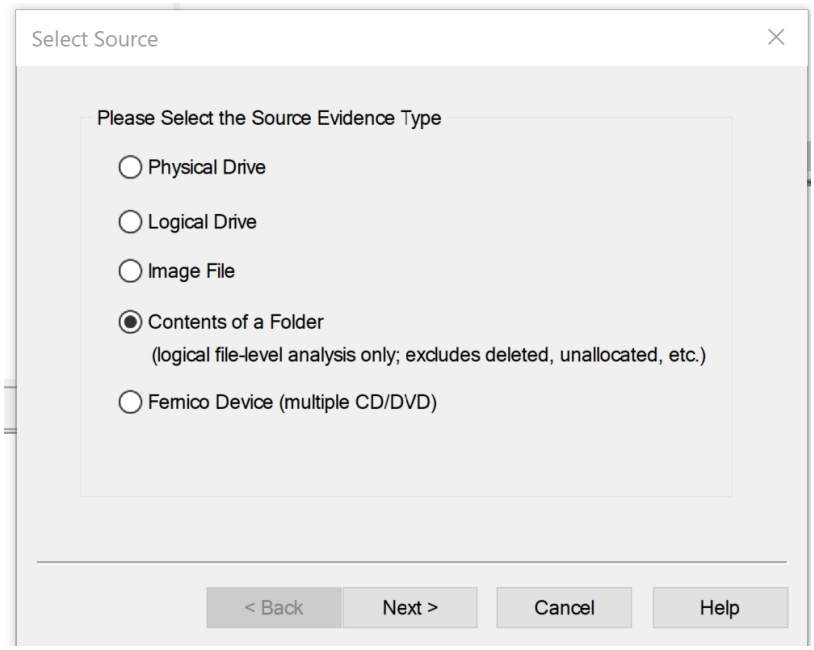
Delete a File from the folder that needs to be recovered later. In this case, delete "Blogging.docx"

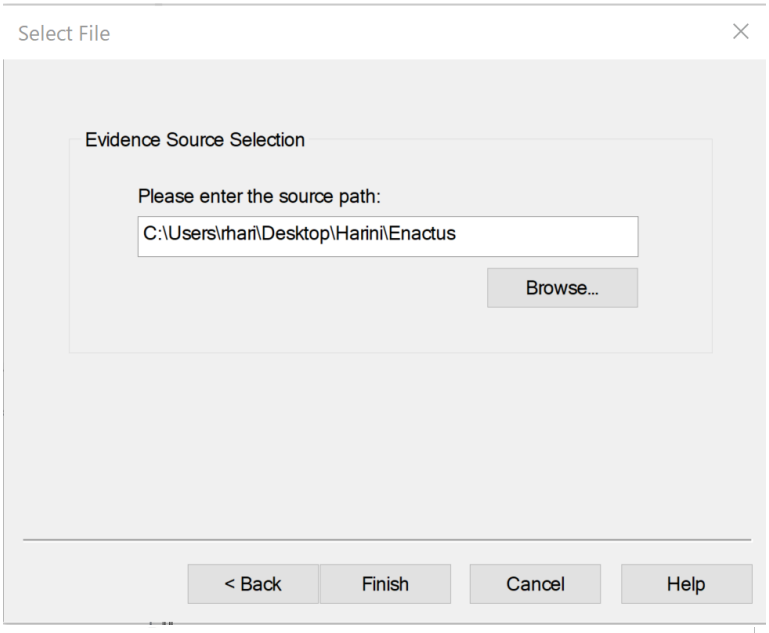
Create an image of the folder using FTK Imager

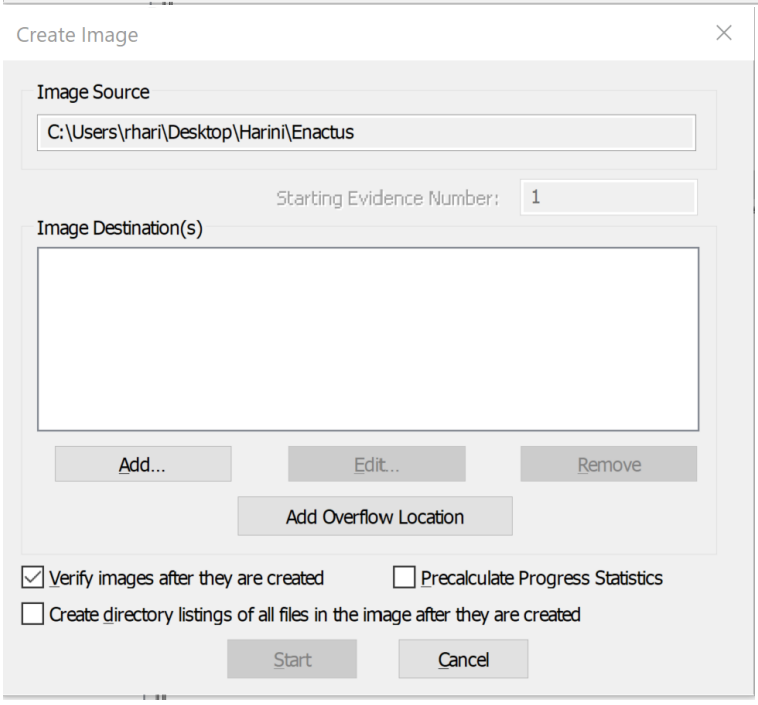
File -> Create Disk Image -> Select Source -> Contents of a Folder -> Enter Image Source Path of the Folder -> Add in Image Destination -> Enter Image Destination Folder and File Name -> Finish -> Start

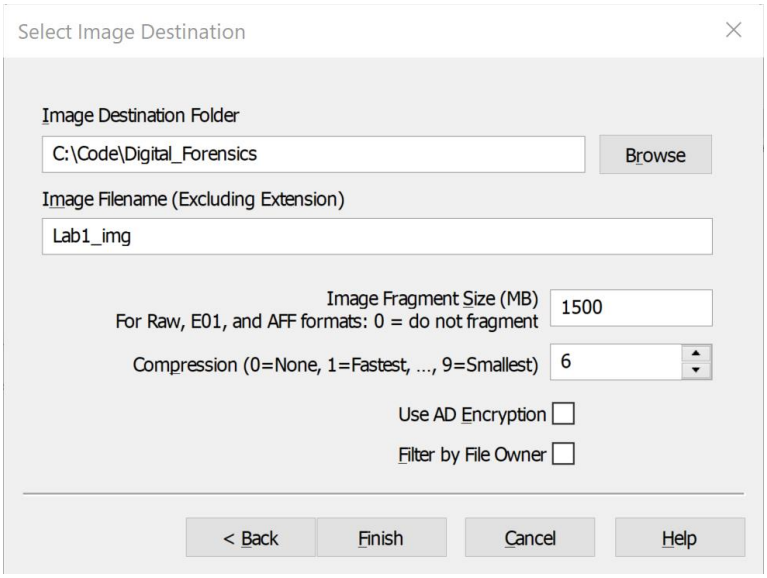
Using RecoverMyFiles, recover deleted file from the Image

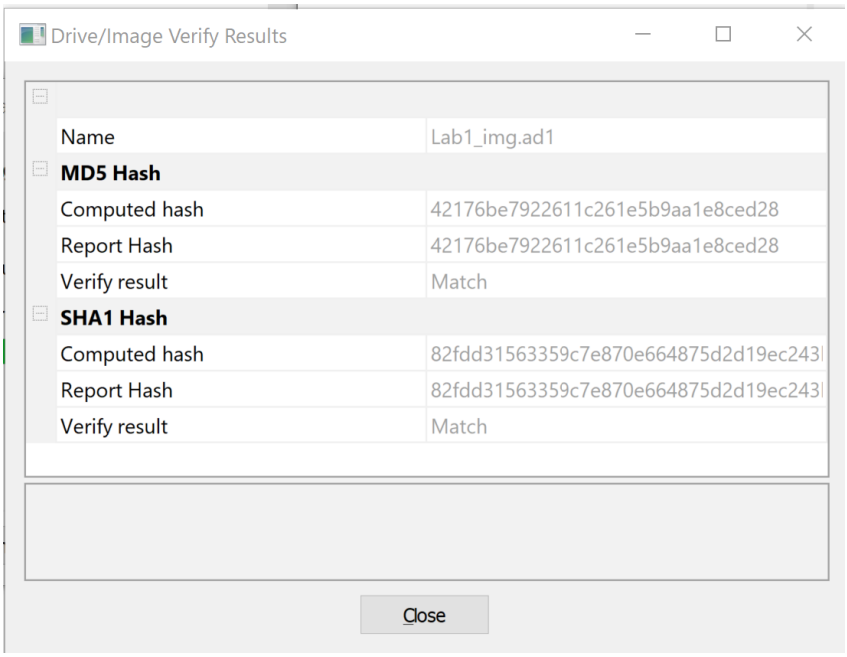
Screenshots:




Select File
Evidence Source Selection
Please enter the source path:
C:\Users\rhari\Desktop\Harini\Enactus
Browse...
< Back
Finish
Cancel
Help


Create Image
Image Source
C:\Users\rhari\Desktop\Harini\Enactus
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel





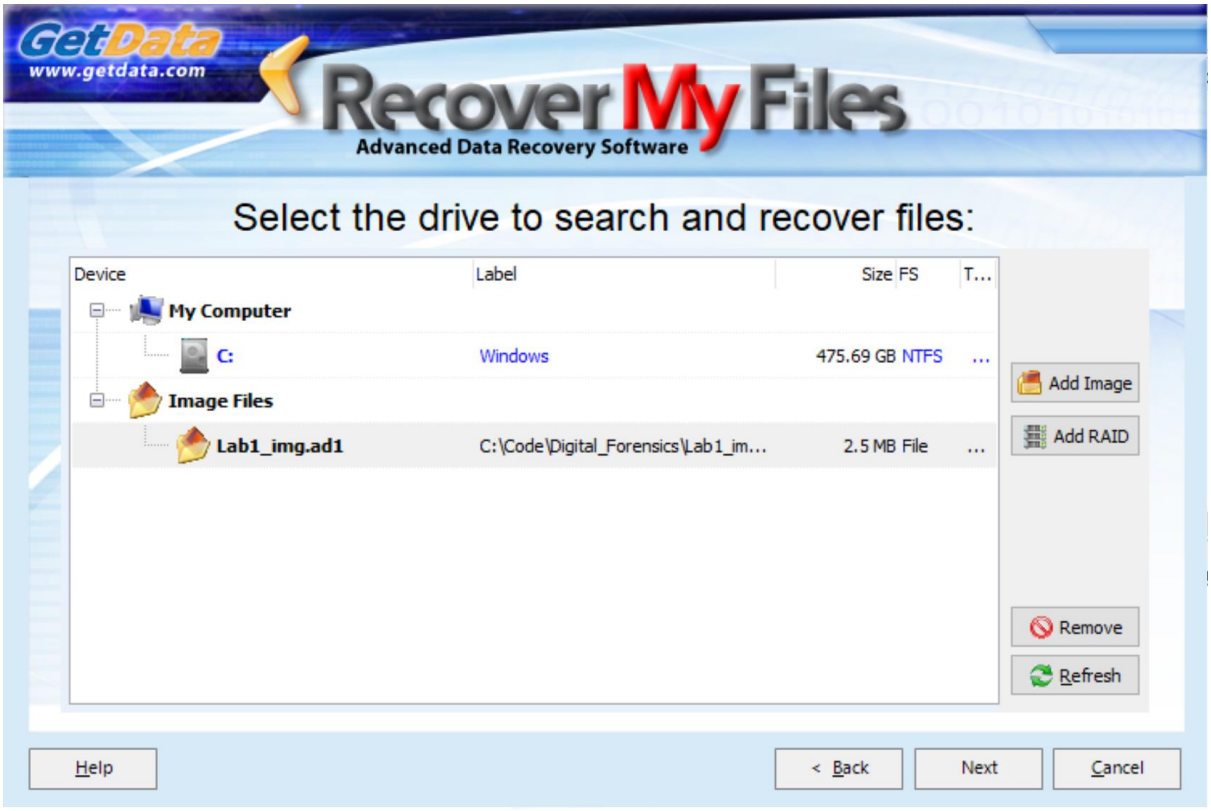
2. Using RecoverMyFiles tool

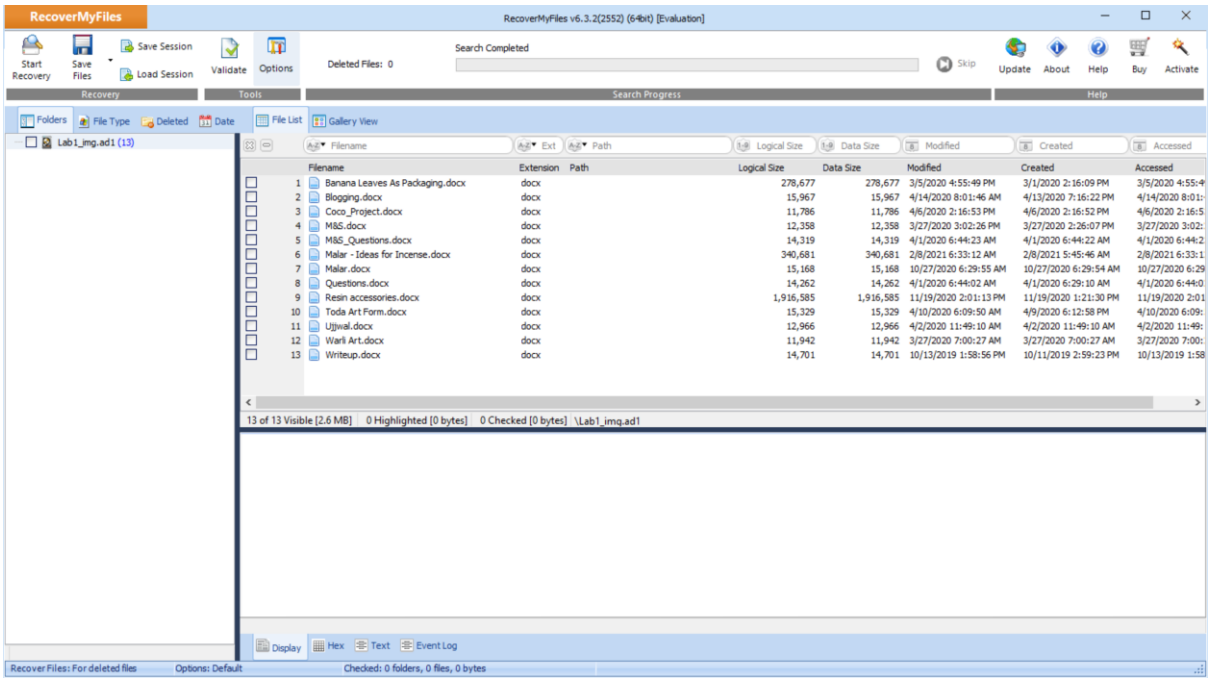
Procedure:

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:


GetData
www.getdata.com
Recover My Files
Advanced Data Recovery Software
Select the drive to search and recover files:
Device
Label
Size
FS
T...
My Computer
C:
Windows
475.69 GB
NTFS
Image Files
Lab1_img.ad1
C:\Code\Digital_Forensics\Lab1_im...
2.5 MB
File
Add Image
Add RAID
Remove
Refresh
Help
< Back
Next
Cancel


RecoverMyFiles
RecoverMyFiles v6.3.2(2552) (64bit) [Evaluation]
Start Recovery
Save Files
Save Session
Load Session
Validate
Options
Deleted Files: 0
Search Completed
Skip
Update
About
Help
Buy
Activate
Recovery
Tools
Search Progress
Help
Folders
File Type
Deleted
Date
File List
Gallery View
Lab1_img.ad1 (13)
Filename
Ext
Path
Logical Size
Data Size
Modified
Created
Accessed
1 Banana Leaves As Packaging.docx docx 278,677 278,677 3/5/2020 4:55:49 PM 3/1/2020 2:16:09 PM
2 Blogging.docx docx 15,967 15,967 4/14/2020 8:01:46 AM 4/13/2020 7:16:22 PM
3 Coco_Project.docx docx 11,786 11,786 4/6/2020 2:16:53 PM 4/6/2020 2:16:52 PM
4 M&S.docx docx 12,358 12,358 3/27/2020 3:02:26 PM 3/27/2020 2:26:07 PM
5 M&S_Questions.docx docx 14,319 14,319 4/1/2020 6:44:23 AM 4/1/2020 6:44:22 AM
6 Malar - Ideas for Incense.docx docx 340,681 340,681 2/8/2021 6:33:12 AM 2/8/2021 5:45:46 AM
7 Malar.docx docx 15,168 15,168 10/27/2020 6:29:55 AM 10/27/2020 6:29:54 AM
8 Questions.docx docx 14,262 14,262 4/1/2020 6:44:02 AM 4/1/2020 6:29:10 AM
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
10 Toda Art Form.docx docx 15,329 15,329 4/10/2020 6:09:50 AM 4/9/2020 6:12:58 PM
11 Ujjwal.docx docx 12,966 12,966 4/2/2020 11:49:10 AM 4/2/2020 11:49:10 AM
12 Warli Art.docx docx 11,942 11,942 3/27/2020 7:00:27 AM 3/27/2020 7:00:27 AM
13 Writeup.docx docx 14,701 14,701 10/13/2019 1:58:56 PM 10/11/2019 2:59:23 PM
13 of 13 Visible [2.6 MB] 0 Highlighted [0 bytes] 0 Checked [0 bytes] \Lab1_img.ad1
Display
Hex
Text
Event Log
Recover Files: For deleted files
Options: Default
Checked: 0 folders, 0 files, 0 bytes

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	84e4ff174c5737f347b729461bb3ccde3f3cb756
SHA-256	e6b393cbb889faa8fe84993ef44c155872c4f7437e213b7bbba2adf55495ec81
SHA-384	c1b37595ac61ce9c703f507aada1e9367ecade9c47997270bfc71aaa3a0269cade25d9eb4de98b01240271411d3cd109
SHA-512	3875413128696d0caef644659983baaccb744603dfdc29d6a3f8adc78ca16325a218c7c27d12e672d886575e105350c6e04b9fe93778ecd9364291d851edc064

MD5: 244ed853d227771b38fe786015b803e

Modified PowerPoint

Hash functions.pptx	(n/a) - 280176 bytes
MD5	1a81781daaa079f414458c5081eebfbf
SHA-1	07cdc2a54633b454c45007e729ad53cebd6ff78c
SHA-256	ff580c6728204790ab07e6c88bd040b56e0951e450d1058ff504786b9f842ca0
SHA-384	060fb8823e1c2989e385427f1657106b76776e7da838a782c467236db335695c5150161734d59790023a77732acd4972
SHA-512	469757646d6555ab2bdcce18bd3d1353263072111f3c6f11045b9957c6b955904d3aed877c166ba82278adff9c88548e40e21efbcfe7fdd1cfc1c1bef38399a8

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-PihI8kTtX-s-unsplash.jpg	(image/jpeg) - 3924249 bytes
MD5	5fd42972609085d2441f47bf191220d5
SHA-1	8fc6190d5050635713748fdd41e4acac05f6a86f
SHA-256	db14e99afdc5d93bacdc180ec3e01d0e402d284cb3275d1d06b824e3a5de48ab
SHA-384	184da9fa794dbd14b7f354f7f53106c44de40be0773ff05376b87d8e4444fb2e5e08a3a69e45a20d2ad265a11c9fff4d
SHA-512	96f45a2117af606d7e013c775a62920c0b610d1a680b726e80a4472b7683a54eebeab73fb87fea4ef5e351fe211e69fd7c79dadbe910e738ee2154acde528cb7

MD5: 5fd42972609085d2441f47bf191220d5

Un-modified Image

joey-kyber-PihI8kTtX-s-unsplash.jpg	(image/jpeg) - 3924249 bytes
MD5	5fd42972609085d2441f47bf191220d5
SHA-1	8fc6190d5050635713748fdd41e4acac05f6a86f
SHA-256	db14e99afdc5d93bacdc180ec3e01d0e402d284cb3275d1d06b824e3a5de48ab
SHA-384	184da9fa794dbd14b7f354f7f53106c44de40be0773ff05376b87d8e4444fb2e5e08a3a69e45a20d2ad265a11c9fff4d
SHA-512	96f45a2117af606d7e013c775a62920c0b610d1a680b726e80a4472b7683a54eebeab73fb87fea4ef5e351fe211e69fd7c79dadbe910e738ee2154acde528cb7

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\CBS\CBS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT LogFileName as LineFromFile FROM C:\Windows\Logs\CBS\C
BS.log
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
-------------------------
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\CBS\CBS.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\CBS\CBS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Index as LineFromFile FROM C:\Windows\Logs\CBS\CBS.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\CBS\CBS.log

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Text as LineFromFile FROM C:\Windows\Logs\CBS\CBS.log
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
------------------------------------------------------------------------------------------------------------------------
---------------
ﾊﾂ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

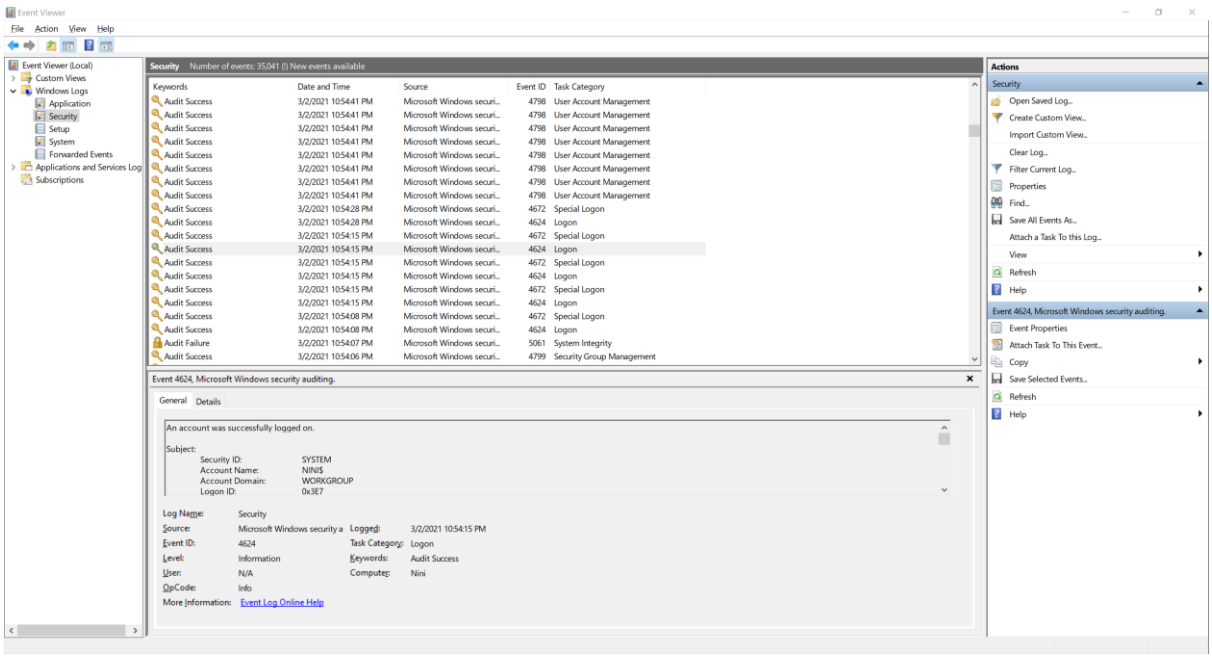
Procedure: Open Event Viewer tool that is inbuilt in the Windows OS

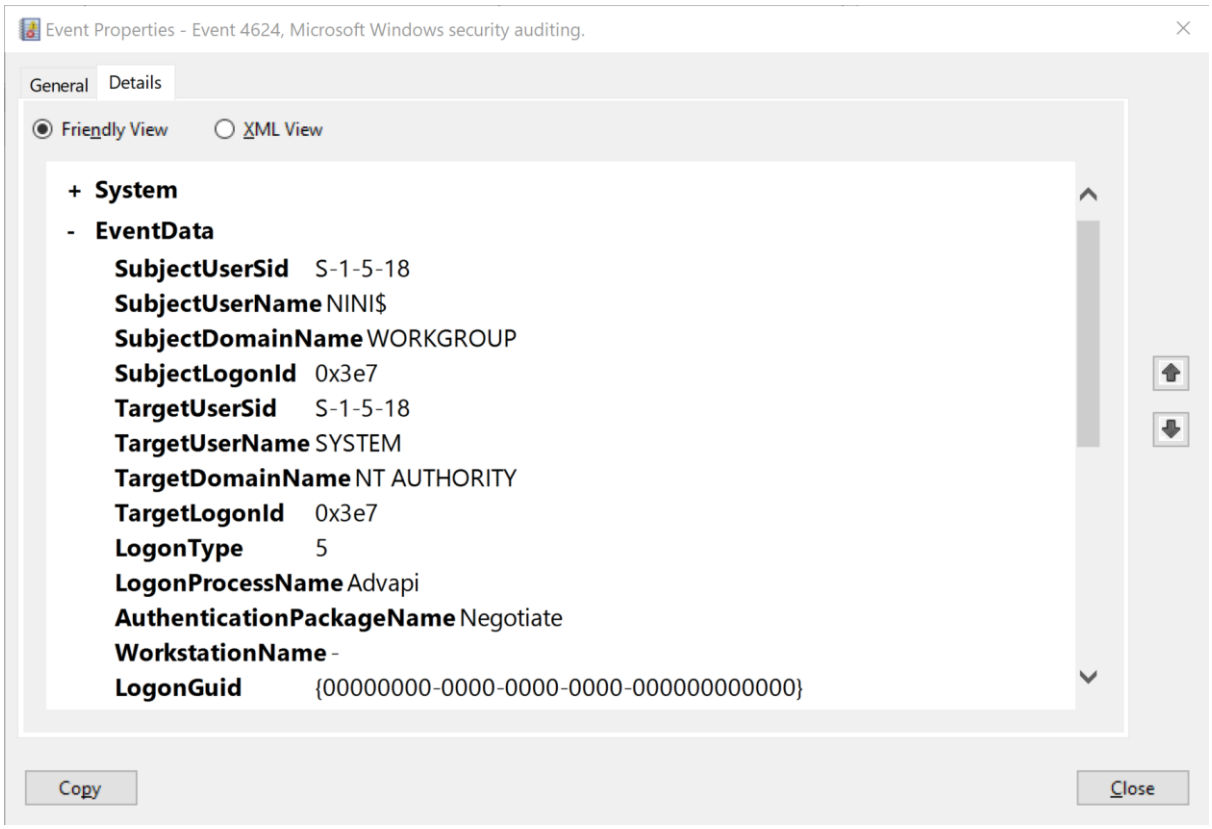
Windows Log -> Security

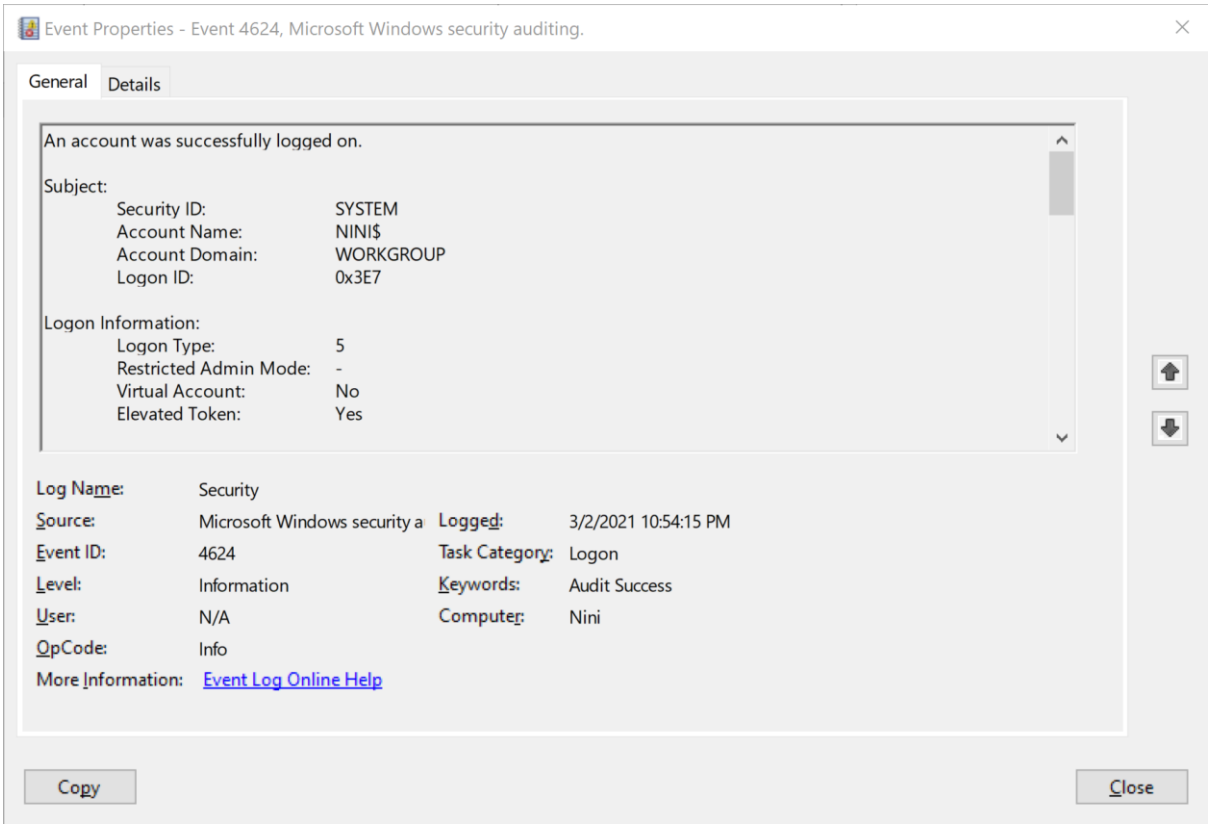
Click on any one Event to view its properties and Details

Event Viewer

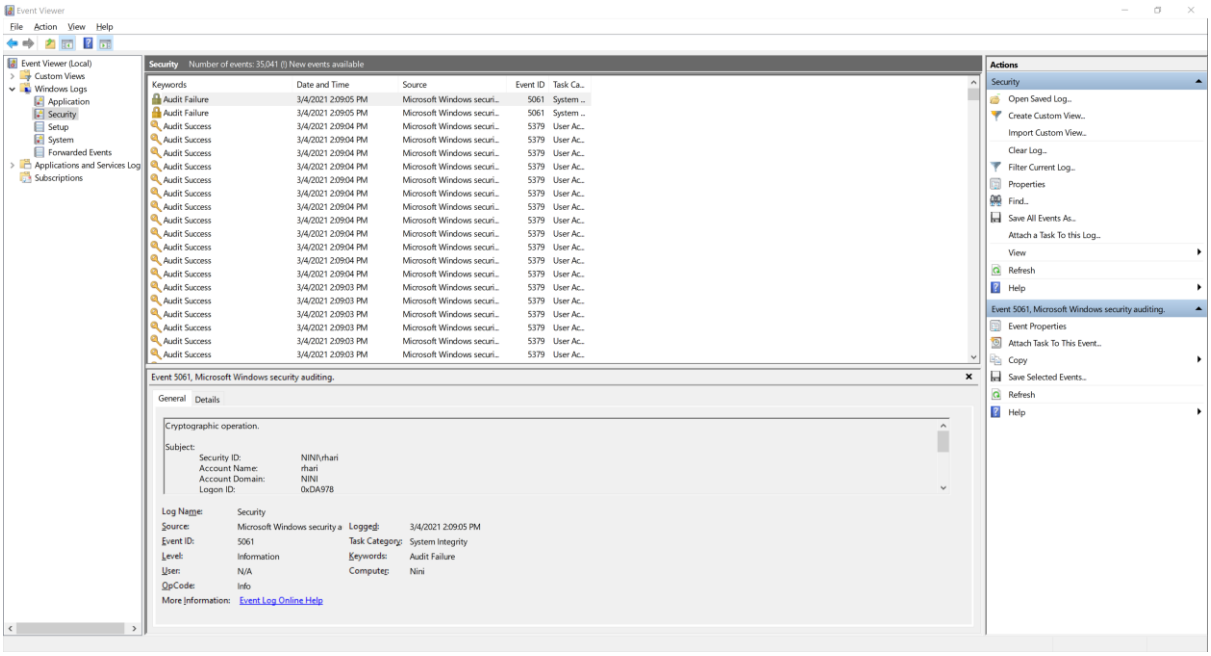
a) Successful Logon

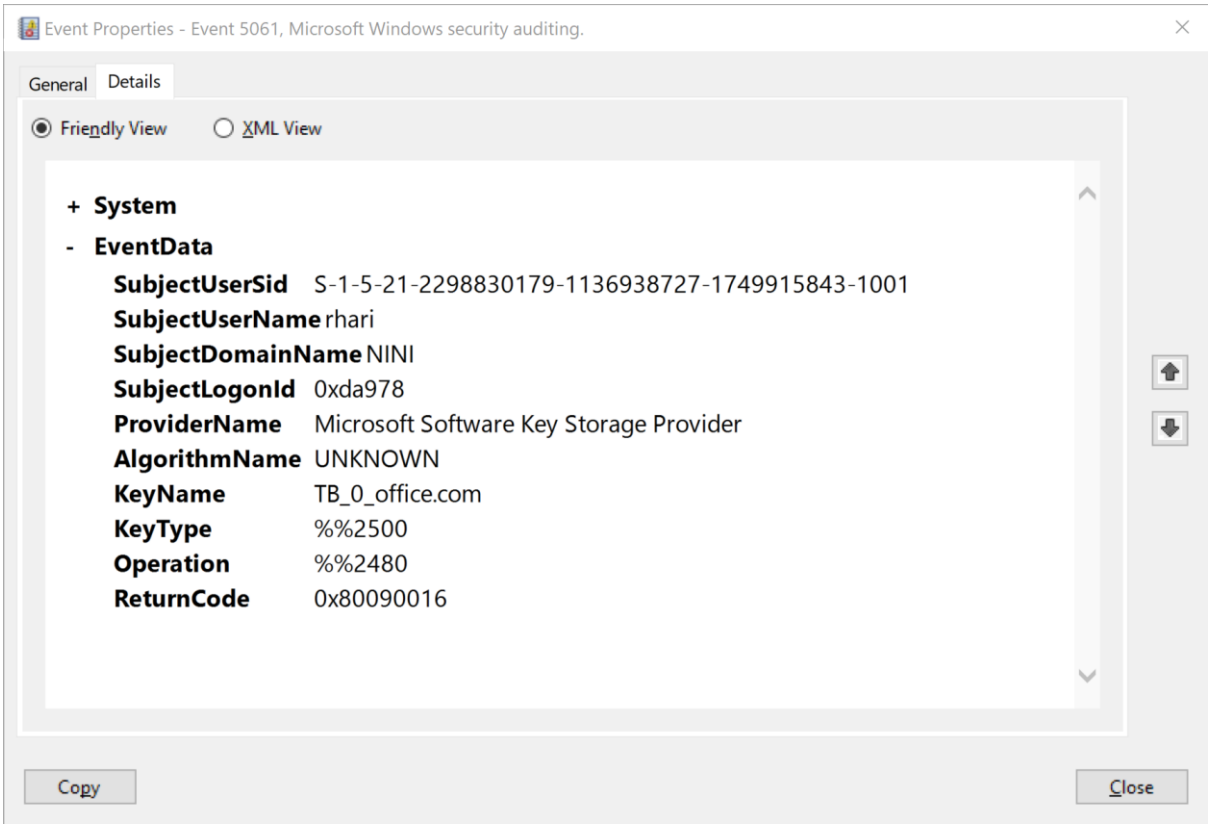


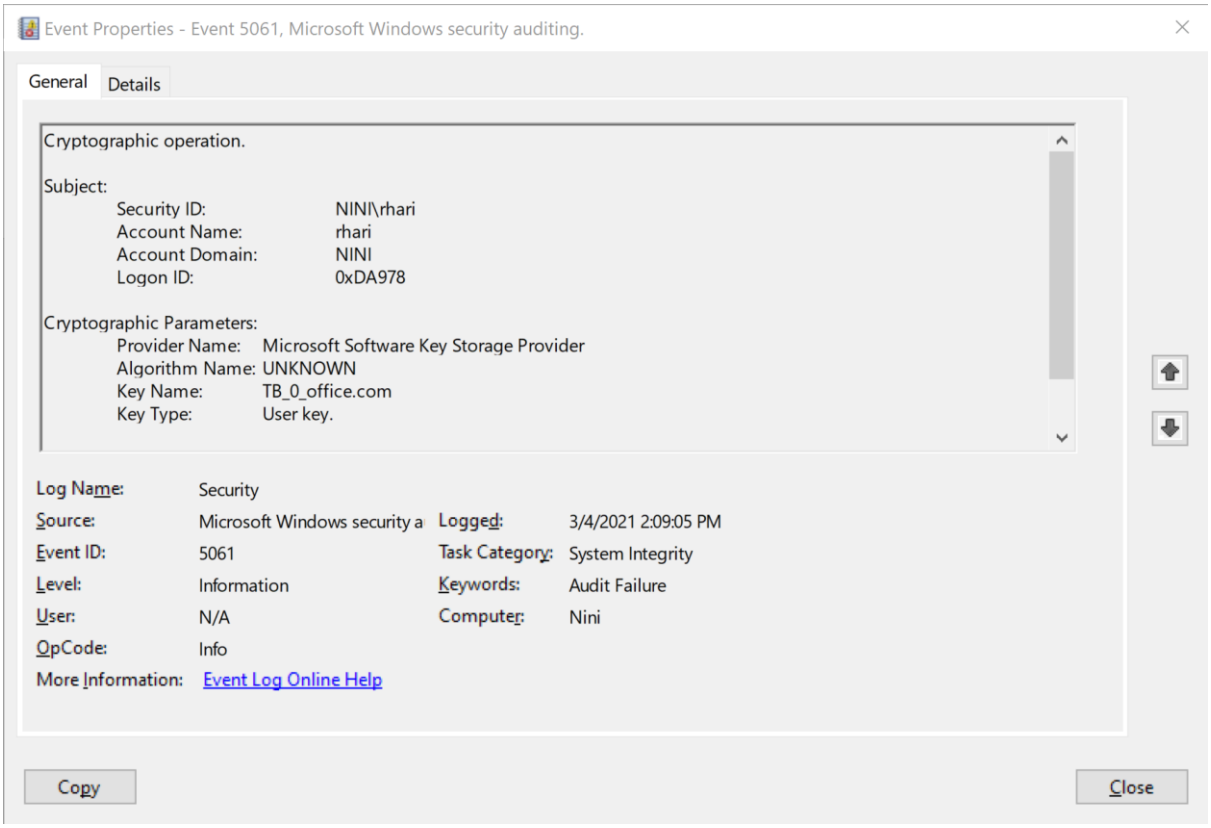




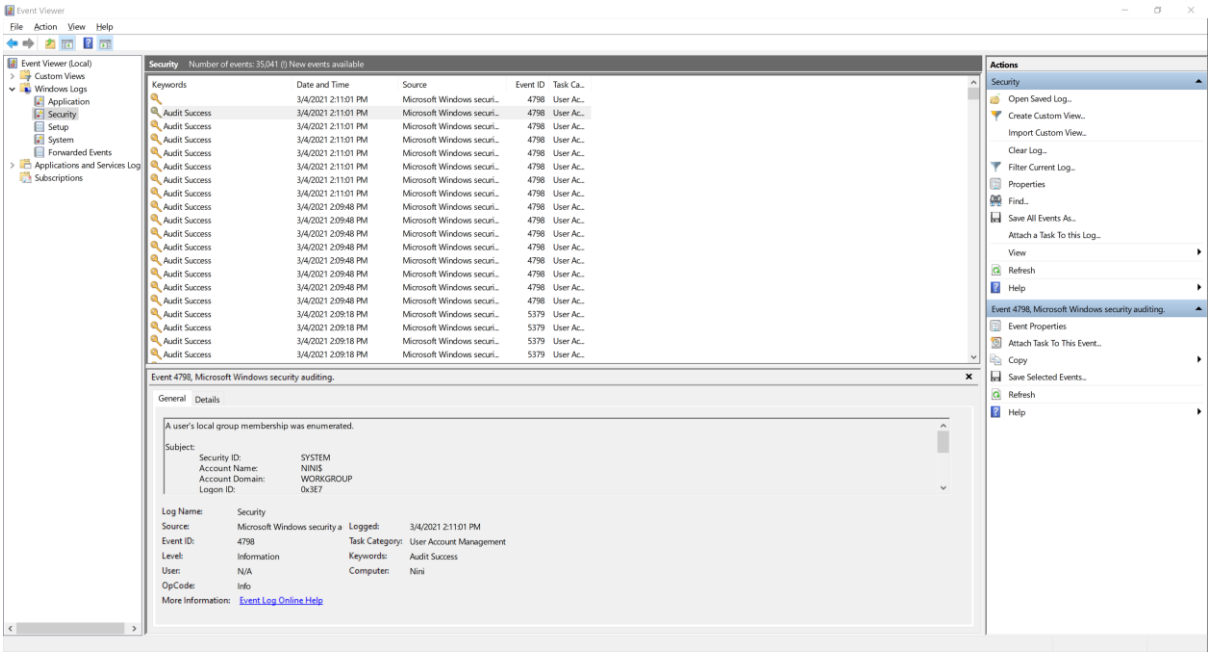
b) Failed logon

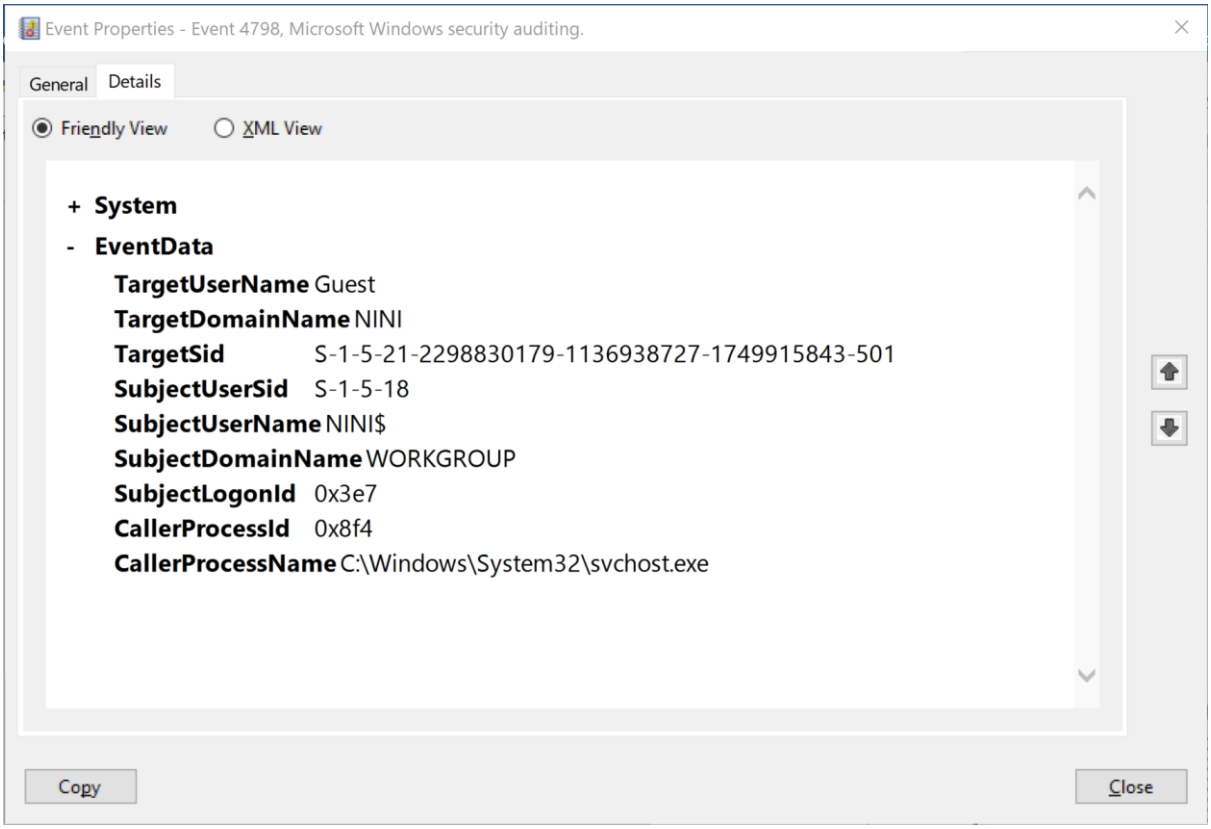


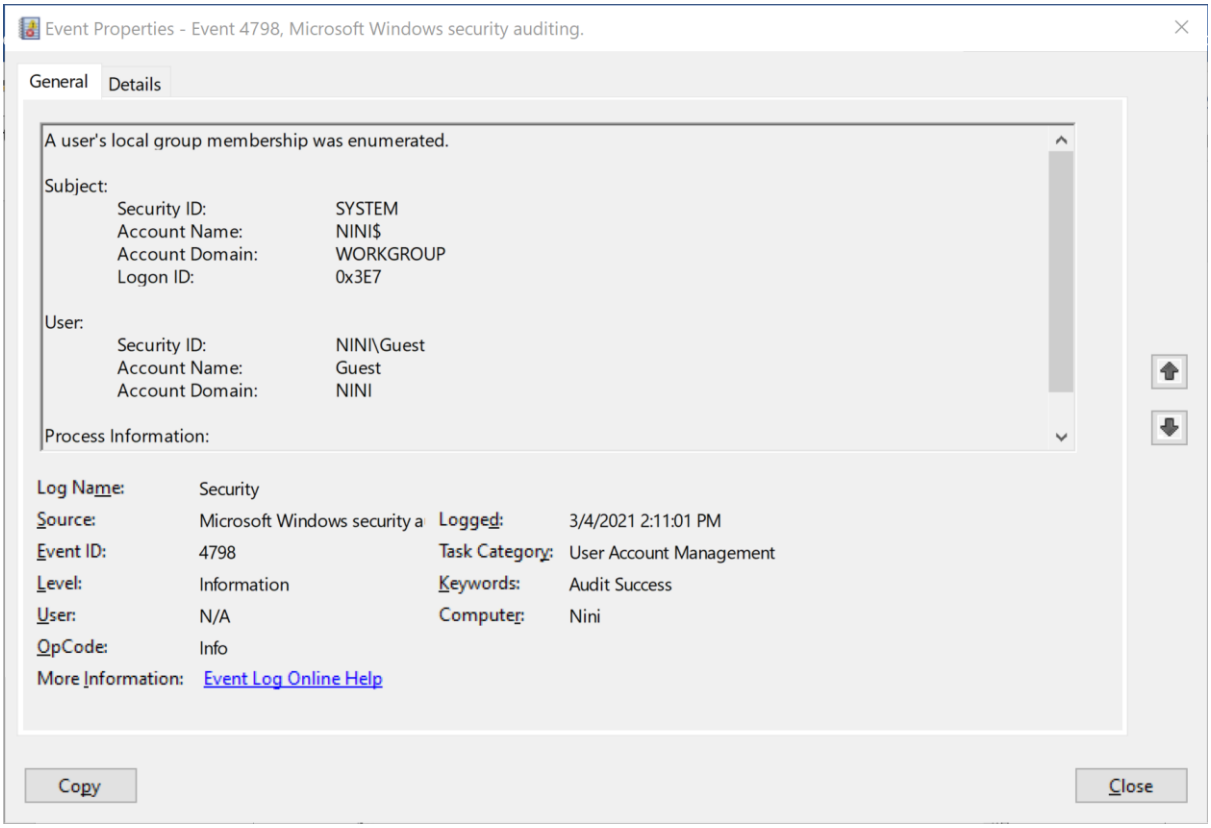




c) A new user was created

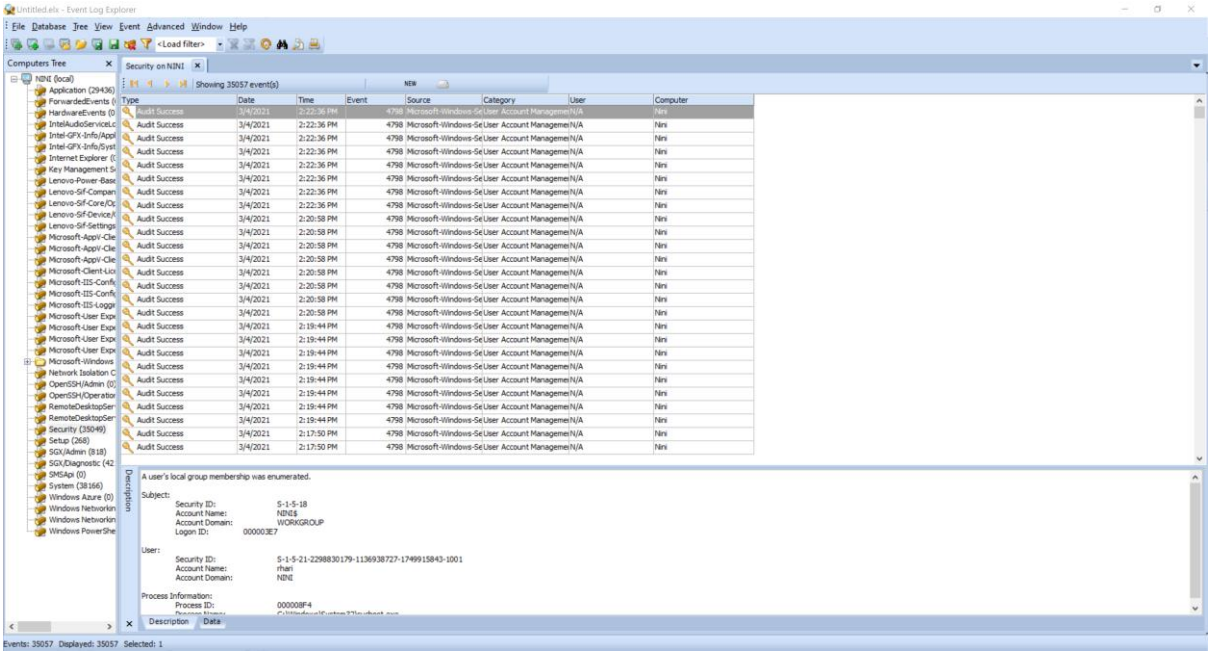

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Security Number of events: 35,041 (!) New events available
Keywords Date and Time Source Event ID Task Ca...
Audit Success 3/4/2021 2:11:01 PM Microsoft Windows securi... 4798 User Ac...
Audit Success 3/4/2021 2:09:48 PM Microsoft Windows securi... 4798 User Ac...
Audit Success 3/4/2021 2:09:18 PM Microsoft Windows securi... 5379 User Ac...
Event 4798, Microsoft Windows security auditing.
General Details
A user's local group membership was enumerated.
Subject:
Security ID: SYSTEM
Account Name: NINI$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security a
Logged: 3/4/2021 2:11:01 PM
Event ID: 4798
Task Category: User Account Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: Nini
OpCode: Info
More Information: Event Log Online Help
Actions
Security
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 4798, Microsoft Windows security auditing.
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

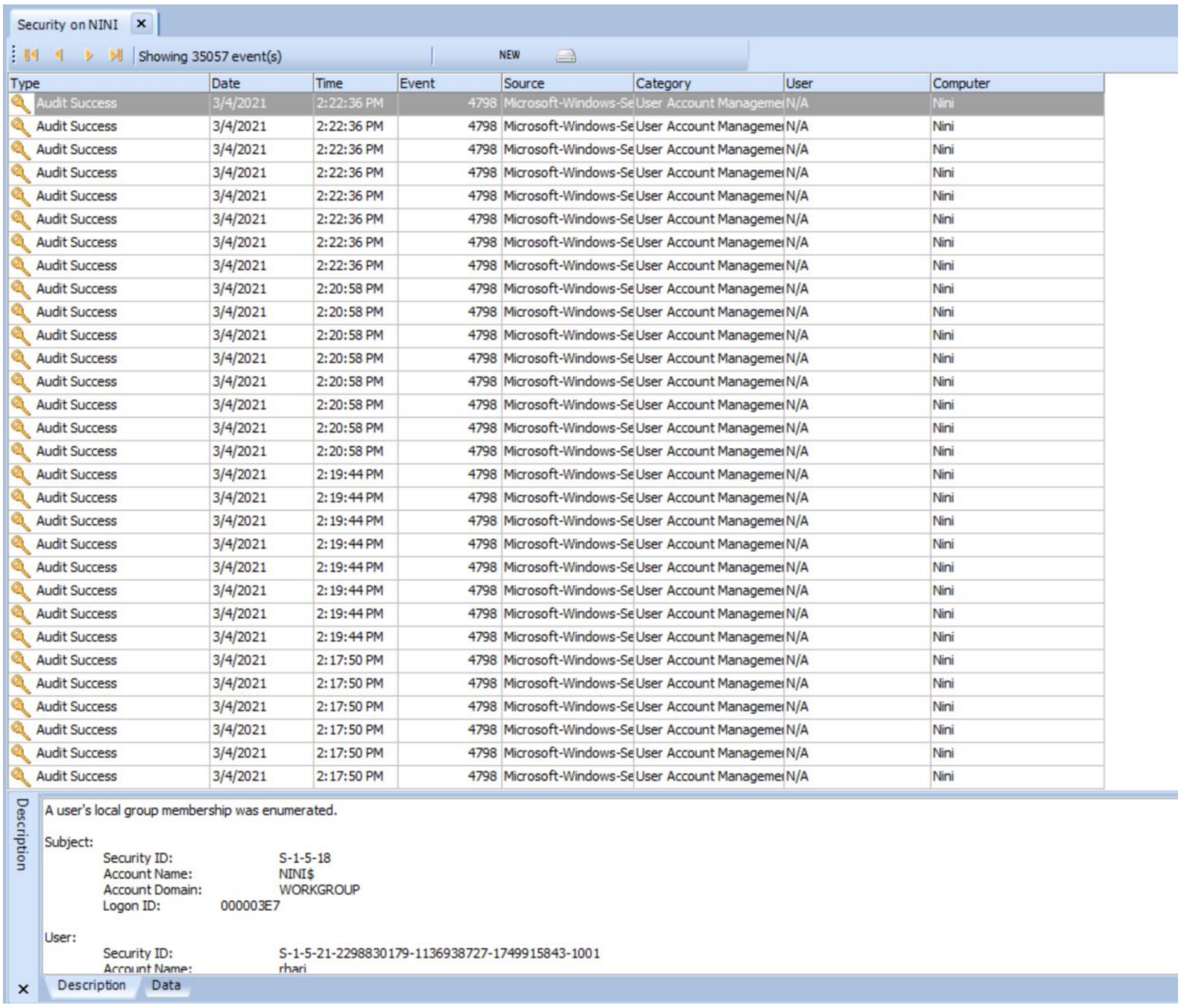

Event Properties - Event 4798, Microsoft Windows security auditing.
General
Details
Friendly View
XML View
+ System
- EventData
TargetUserName Guest
TargetDomainName NINI
TargetSid S-1-5-21-2298830179-1136938727-1749915843-501
SubjectUserSid S-1-5-18
SubjectUserName NINI$
SubjectDomainName WORKGROUP
SubjectLogonId 0x3e7
CallerProcessId 0x8f4
CallerProcessName C:\Windows\System32\svchost.exe
Copy
Close



Event Log Explorer Tool

a) Successful Logon





Security on NINI

Showing 35057 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:22:36 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:20:58 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:19:44 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini
Audit Success	3/4/2021	2:17:50 PM	4798	Microsoft-Windows-Se	User Account Manageme	N/A	Nini

Description

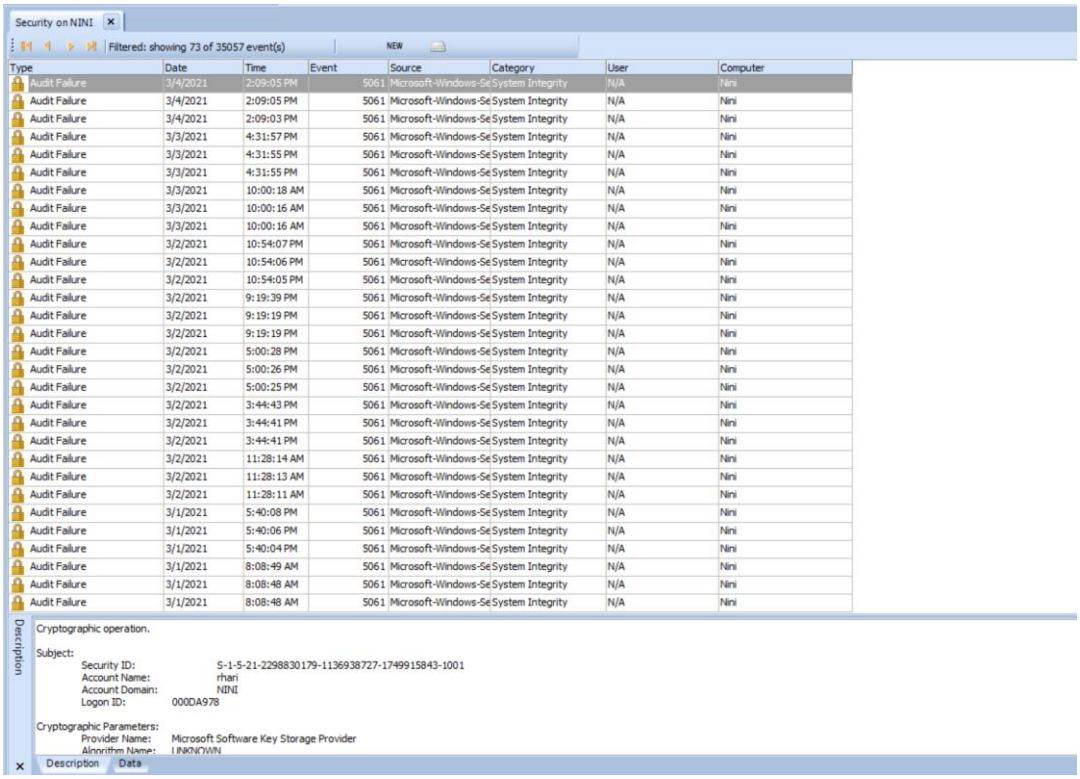
A user's local group membership was enumerated.

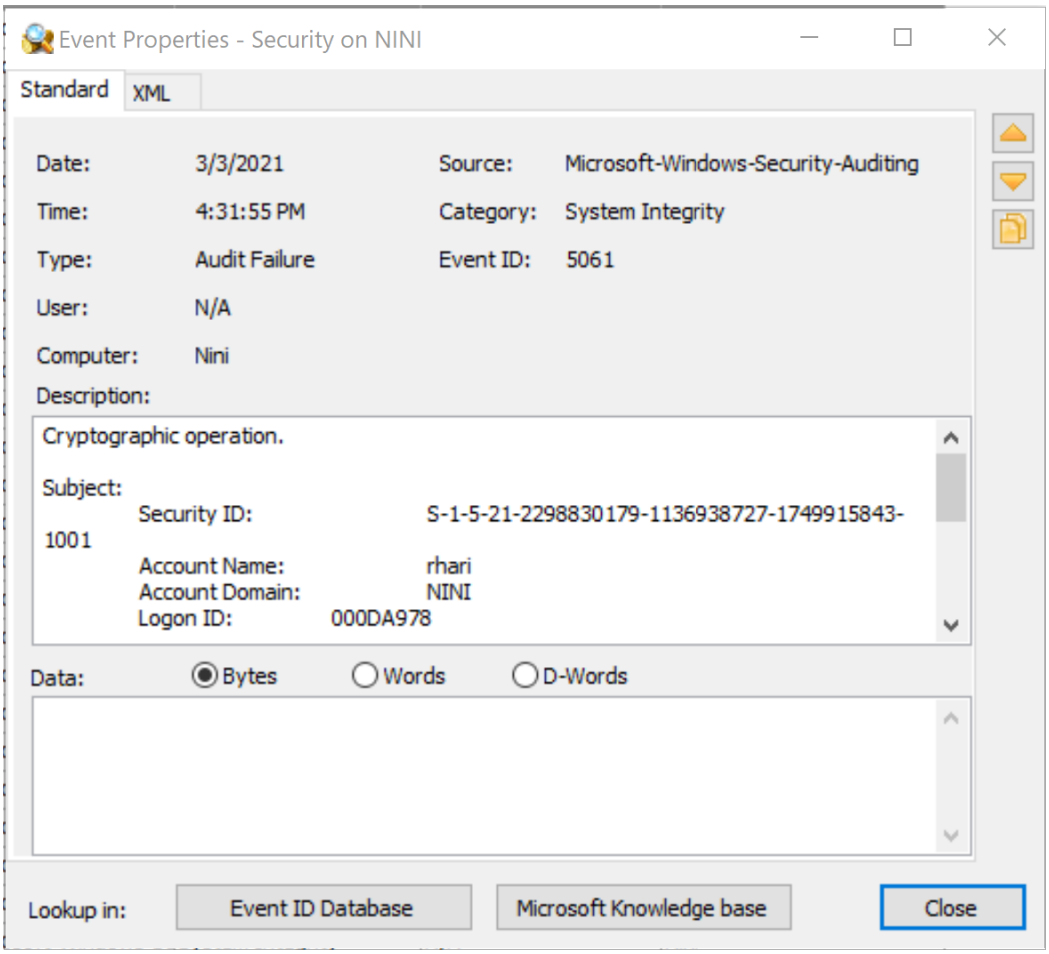
Subject:
Security ID: S-1-5-18
Account Name: NINI$
Account Domain: WORKGROUP
Logon ID: 000003E7

User:
Security ID: S-1-5-21-2298830179-1136938727-1749915843-1001
Account Name: rhari

Description Data

b) Failed logon



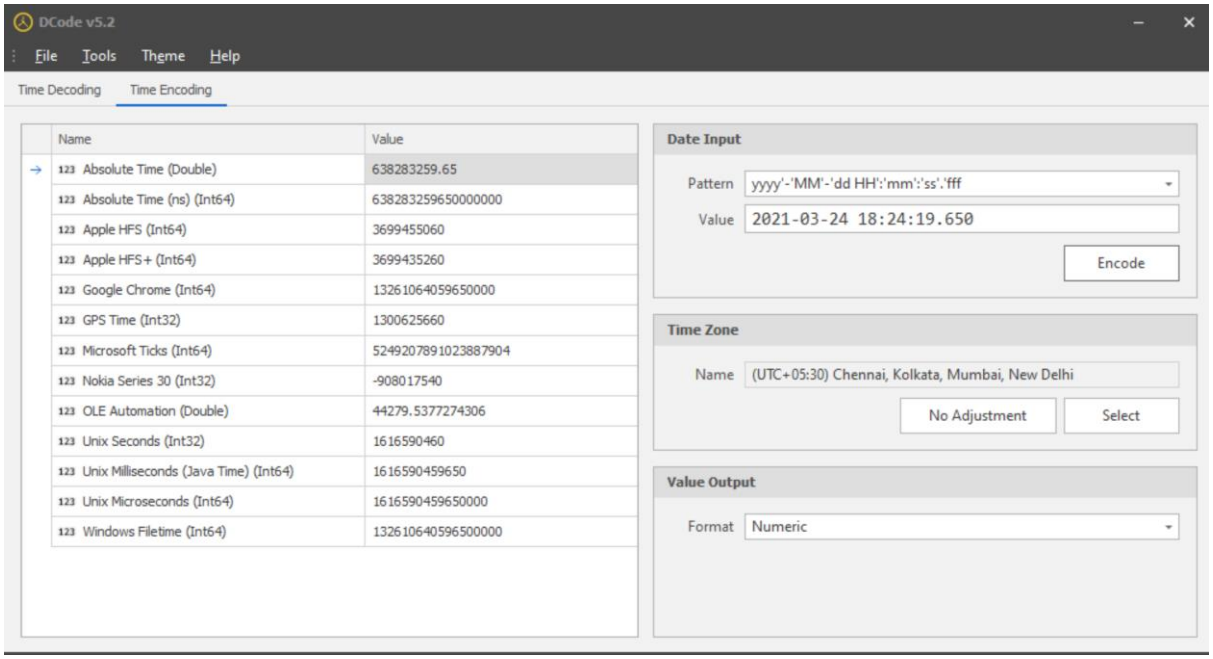


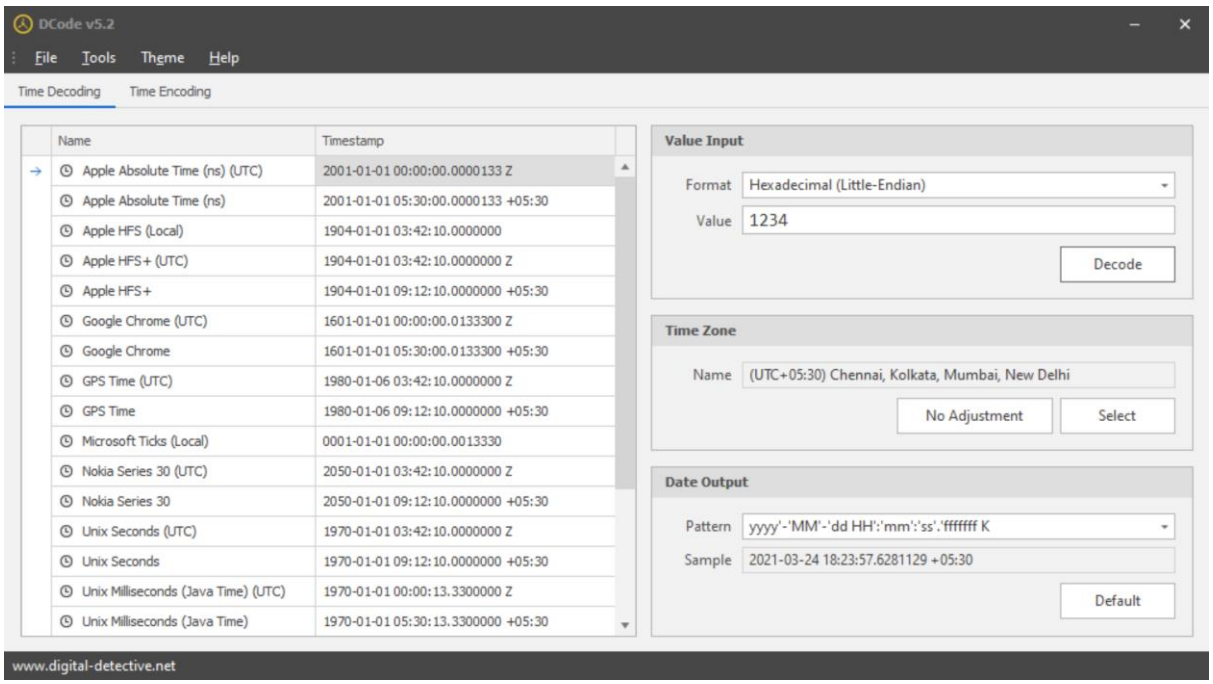
Lab 5: Encoding and Decoding using DCode

R. Harini

18BCE1010

1) Using DCode Tool





2) Using String.exe

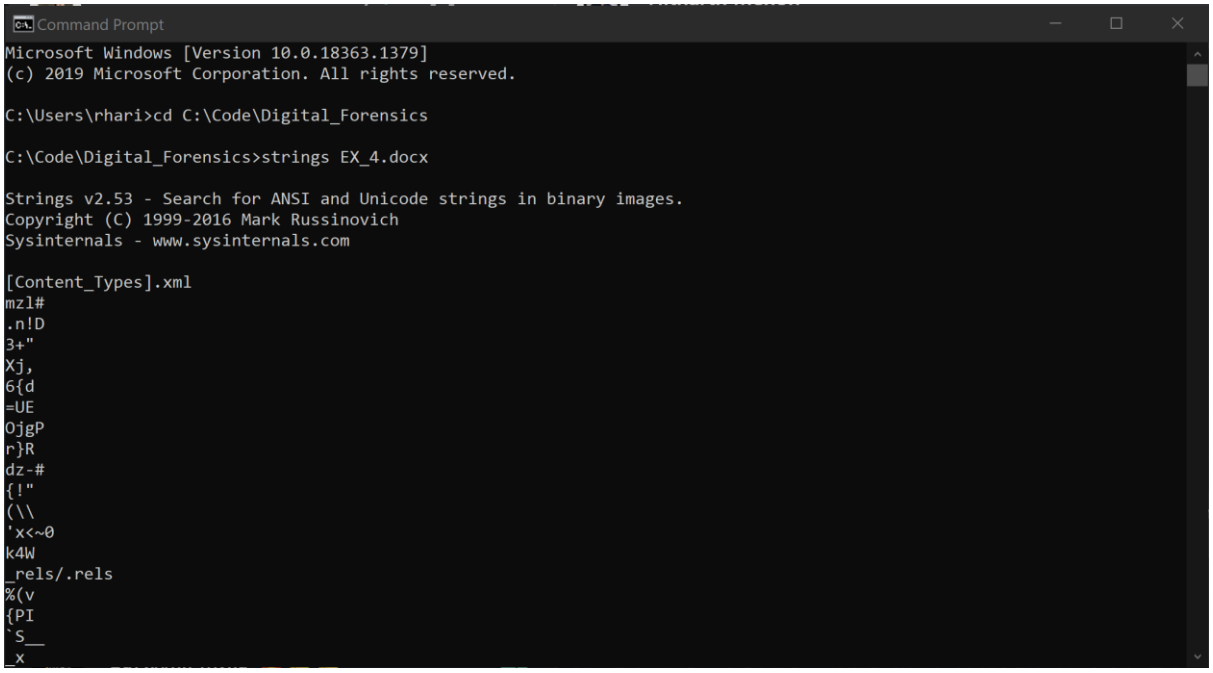
Procedure:

Open cmd

Navigate to the path with the .docx file

Type **strings <filename>.docx**

Output:



Lab 6: Using Windows CMD line

R. Harini

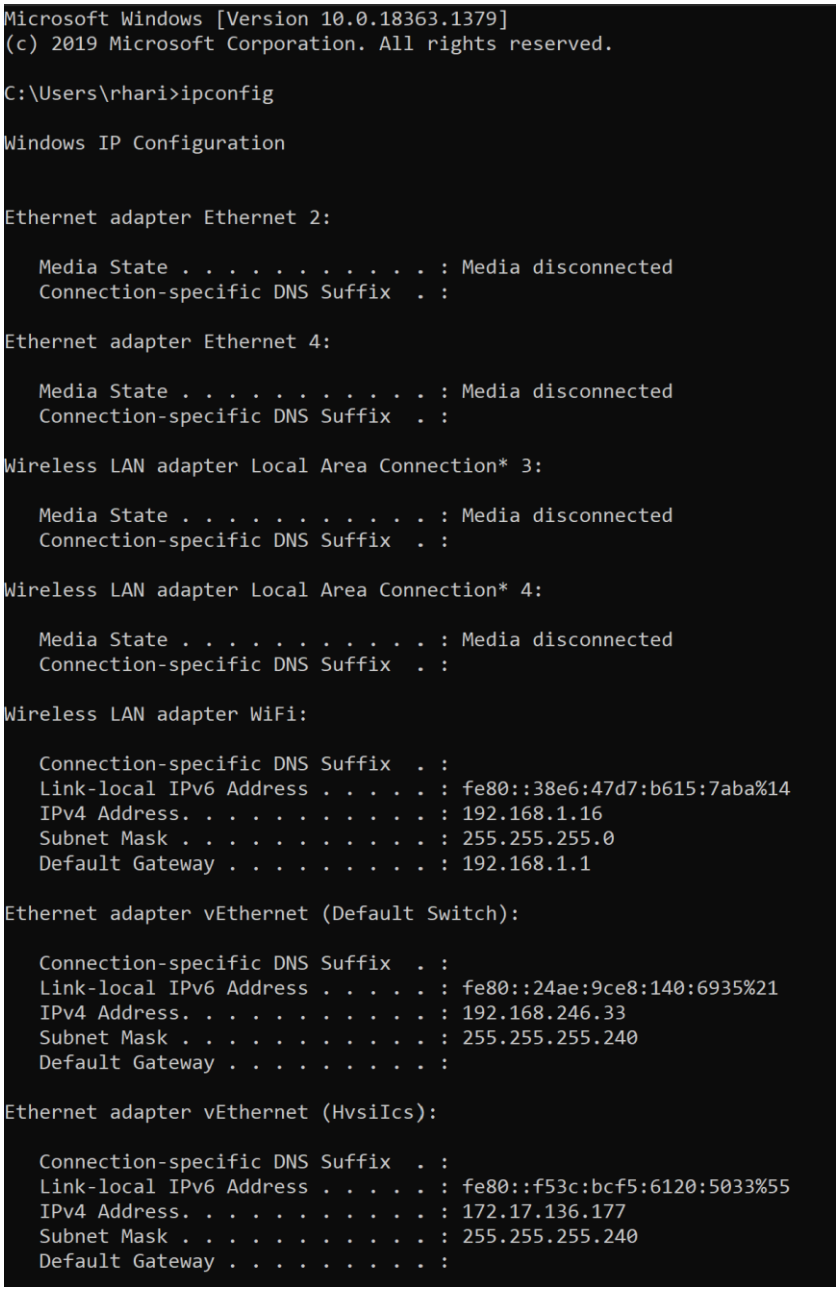
18BCE1010

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



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.
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.
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    127.0.0.1:46624        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              *:*
```