



---

# FACT

Forensic Artifact Comprehensive Triage

Designed To Help FORENSIC Professional To ACT Smartly

---



## Acknowledgments: Fellow Explorers in the Quest for Facts

We are grateful to acknowledge the invaluable contributions of existing digital forensic tools that served as inspiration for the foundation of our own tool ***“FACT – Designed to help FORENSIC professional to ACT Smartly”***.

We extend our sincere appreciation to the creators and developers of Arsenal-Image-Mounter, CyLR, Kape, RegRipper, TimelineExplorer and special thanks to Eric Zimmerman for his invaluable contributions through his tools. We also extend our apologies if there are any tools or creators we may have missed.

We also express gratitude to the broader community of Digital Forensic & Incident Response practitioners who have shared knowledge, provided feedback, and collaborated in various capacities. Together, we have built upon the collective wisdom and experience to create a new tool that we believe will make meaningful contributions to the field of Digital Forensic.

## Contents

<b>Acknowledgments: Fellow Explorers in the Quest for Facts .....</b>	<b>2</b>
<b>Introduction: Unlocking Efficiency of FACT .....</b>	<b>4</b>
<b>Exciting Updates in Version 1.2 .....</b>	<b>5</b>
<b>Essential Setup: Ready, Steady &amp; Analyse with Investigative Arsenal.....</b>	<b>6</b>
<b>Deciphering Clues.....</b>	<b>7</b>
<b>Detective's Handbook: Troubleshooting Common Dilemmas.....</b>	<b>16</b>

## Introduction: Unlocking Efficiency of FACT

FACT is a cutting-edge forensic tool designed to revolutionize digital investigation and to help FORENSIC examiner to ACT Smartly. FACT is designed to automate repetitive tasks and reduces the examiner efforts and expedite the investigation by extracting vital artifacts from a mounted device, and there after apply advanced intelligence to uncover details.

The functionality of FACT extends well beyond expediting investigations; it provides a wealth of essential details about the target device, including Host-name, IP-Address, Domain Accounts, Local Accounts, and many more. One of its standout features is the ability to construct a comprehensive timeline of events, offering a crystal-clear chronology of activities on the target device. And it doesn't stop there! FACT demonstrates its expertise by thoroughly examining Registry artifacts and Event log Artifacts, revealing crucial insights that might otherwise go unnoticed.

Having FACT at your fingertips enables you to access a wealth of information, giving you the edge to navigate the digital evidence with top-notch efficiency and smarts.

## Exciting Updates in Version 1.2

Whether you're conducting Incident Response or Digital Forensics, correlating findings across multiple artifacts is crucial, and the new "FACT Magic" module in Version 1.2 simplifies this process. For example, you might identify an RDP connection from a specific IP address (X.Y.Z.W) in event logs, followed by spotting a "Mimikatz" entry in the Master File Table. Further investigation could reveal the presence of MIMIKATZ.EXE-<hash>.pf in the Prefetch. The updated FACT Magic module automates the correlation of such findings, helping you build a timeline that ties critical events together in one click.

This streamlined module allows you to input a specific date range and quickly surface any suspicious or anomalous activity within that timeframe, empowering faster, more precise analysis. Whether you're handling a live response or performing in-depth forensics, FACT Magic enhances efficiency by transforming tedious manual tasks into an automated process, giving you the insights you need to take action quickly

## Essential Setup: Ready, Steady & Analyse with Investigative Arsenal

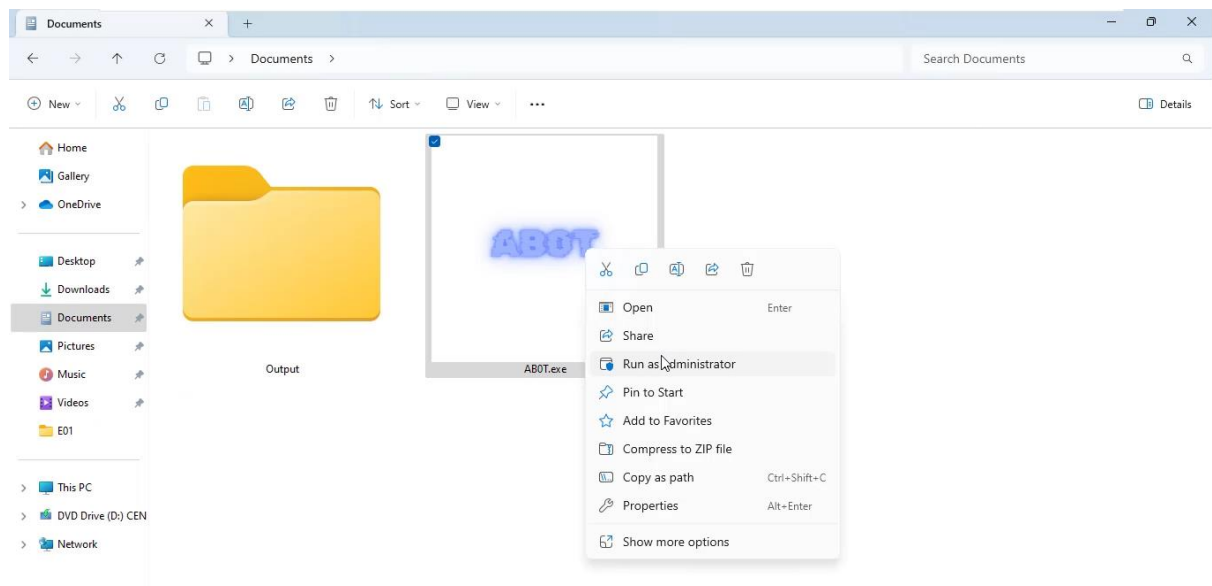
FACT requires fulfilling of the following prerequisites for successful execution.

- Begin by mounting your target Windows disk image (E01/DD) using the "Arsenal Image Mounter."
- Next, simply execute the FACT application as Administrator.

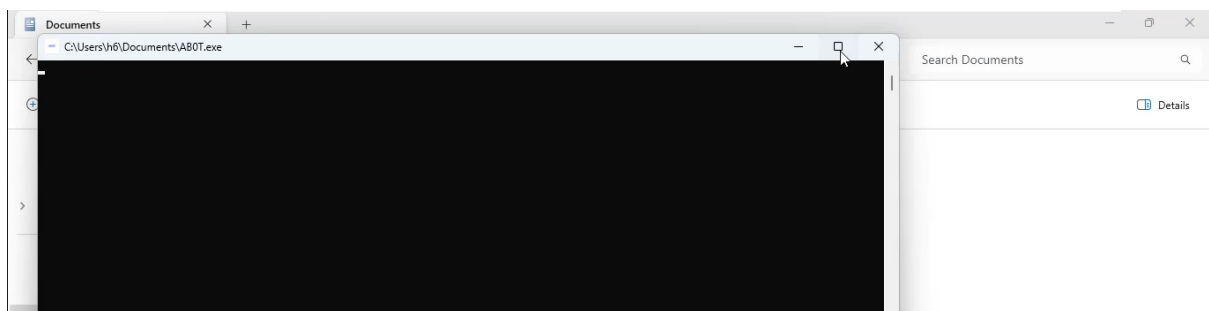
*Note: Always ensure that the targeted Windows disk image is mounted using Arsenal Image Mounter for optimal performance and reliability.*

## Deciphering Clues

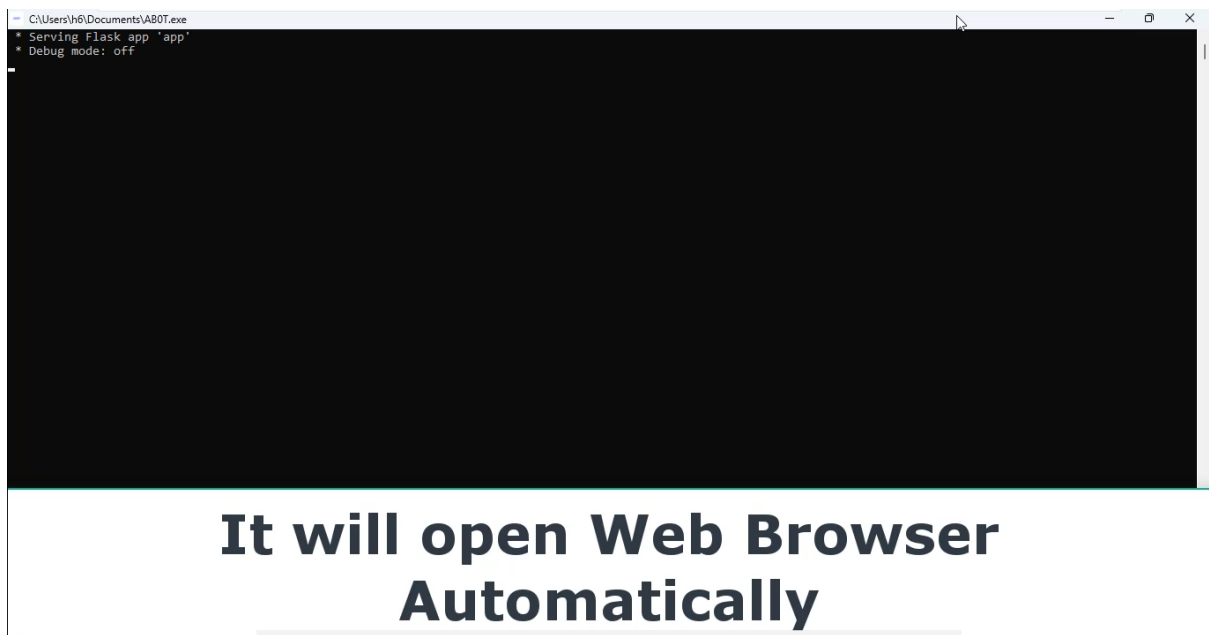
1. Run executable FACT.exe with administrative privileges.



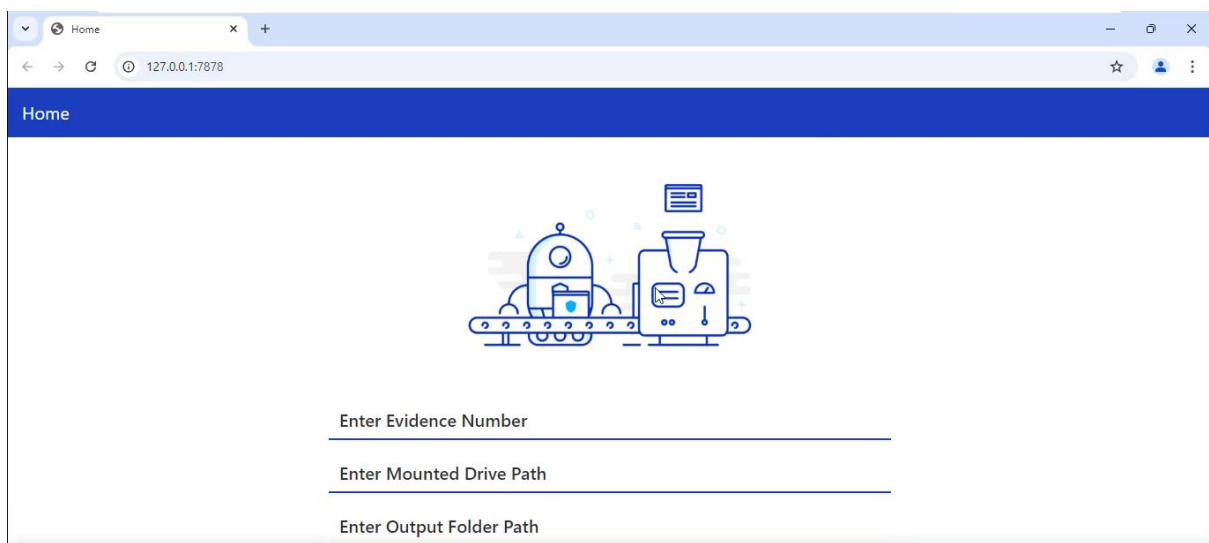
2. Wait for 1-2 minutes for the FACT interface to appear.



3. You will see below screen when loading is going on.



4. Once loading will be completed you will be automatically navigated to the browser window as shown below.

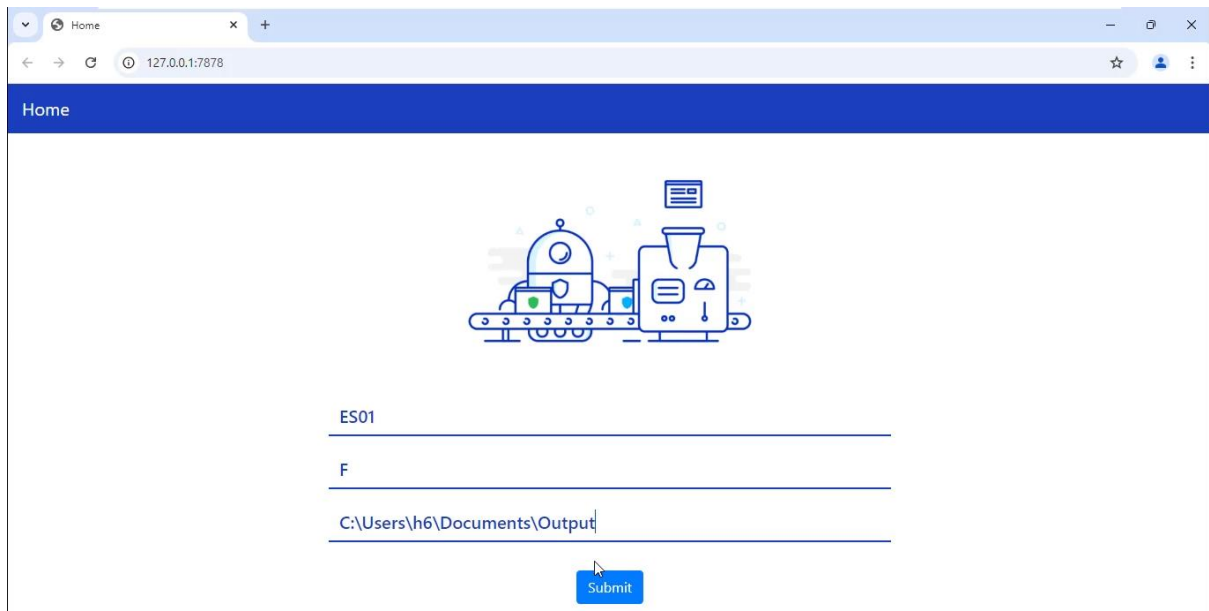


*Ensure that port 7878 is not in use by any other application to prevent conflicts.*



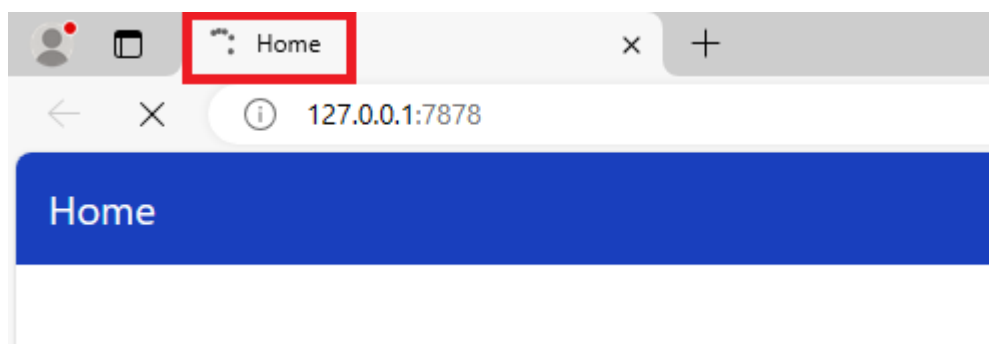
5. On the interface, provide the following details:

- a. Evidence Number
- b. Mounted Drive Letter (e.g., E)
- c. Output Path



The screenshot shows a web browser window with a single tab titled "Home". The address bar displays "127.0.0.1:7878". The page has a blue header with the word "Home". Below the header is a large white area containing a stylized illustration of a laboratory or industrial machine. Underneath the illustration are three input fields. The first field contains the text "ES01". The second field contains the text "F". The third field contains the text "C:\Users\h6\Documents\Output". Below these fields is a blue button labeled "Submit".

6. Click on the "Submit" button after entering the required information.
7. Wait patiently for processing to complete, which may take 15-20 minutes depending on the size of the evidence or image.
8. During processing, observe the animated icon at the top left corner of the tab to indicate that the operation is ongoing.



9. Additionally, check FACT.exe terminal and you will see the progress updates.

```
- Processing chunk 12 of 16 % complete: 75.00% Records found: 1,640
* Serving Flask app 'app'
* Debug mode: off
Collection Started
Please Wait 600 seconds, Collection is going on
Please Wait - 300 Seconds, Collection is going on
```

10. Once processing is finished, you will see "Collection END" on terminal screen and on web browser you will be redirected to Dashboard page.

```
- Total execution time: 1,134.8545 seconds
* Serving Flask app 'app'
* Debug mode: off
Collection Started
Please Wait 600 seconds, Collection is going on
Please Wait - 300 Seconds, Collection is going on
Please Wait - 180 Seconds, Collection is going on
Please Wait - 30 Seconds, Collection is going on
Collection End
```

**As soon as you see "Total Execution Time" you can switch back to web browser. Processing is completed.**



11. Now Click on Basic Details to uncover the basic information from the mounted evidence.

The screenshot shows a web browser window with the address bar displaying "127.0.0.1:7878/BasicDetails". The page has a blue header with "Home" and a "Back" button. The main content area is divided into two panels. The left panel, titled "User Accounts", lists several accounts: Administrator, Guest, DefaultAccount, WDAGUtilityAccount, and Domain Accounts starts now. It also shows the Path: %systemroot%\system32\config\systemprofile and SID: S-1-5-18. The right panel, titled "Details", shows a table of system information:

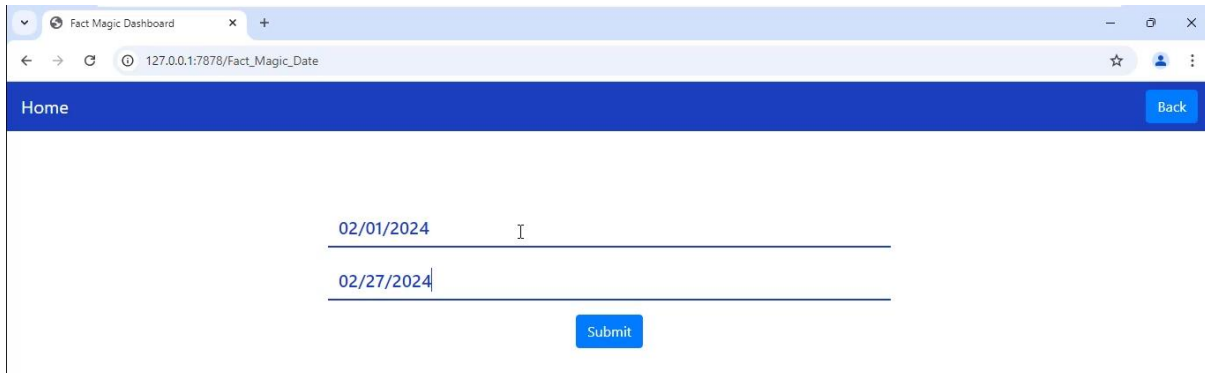
Details	Output
ComputerName	WIN-NI9FBK23SLO
Last Shutdown	2024-02-09 22:56:32Z
Time Zone	GMT Standard Time
OS & Version	Windows Server 2022 Standard
ReleaseID	2009
InstallDate	2023-09-24 21:08:08Z
InstallTime	2023-09-24 21:08:08Z
IP ADDRESS	10.44.0.12

The Windows taskbar is visible at the bottom, showing the Start button, task view, and several application icons. The system tray on the right shows the language as "ENG IN", the time as "13:12", and the date as "15-09-2024".

12. Further, from the dashboard click on “FACT Magic” and you will be redirected to below screen.

The screenshot shows a web browser window with the address bar displaying "127.0.0.1:7878/Fact\_Magic\_Date". The page has a blue header with "Home" and a "Back" button. The main content area is white and contains two input fields for dates. The first field is labeled "Please Enter Start Date (Format: MM/DD/YYYY | 05/21/2023)" and the second field is labeled "Please Enter END Date (Format: MM/DD/YYYY | 05/21/2023)". Below these fields is a blue "Submit" button.

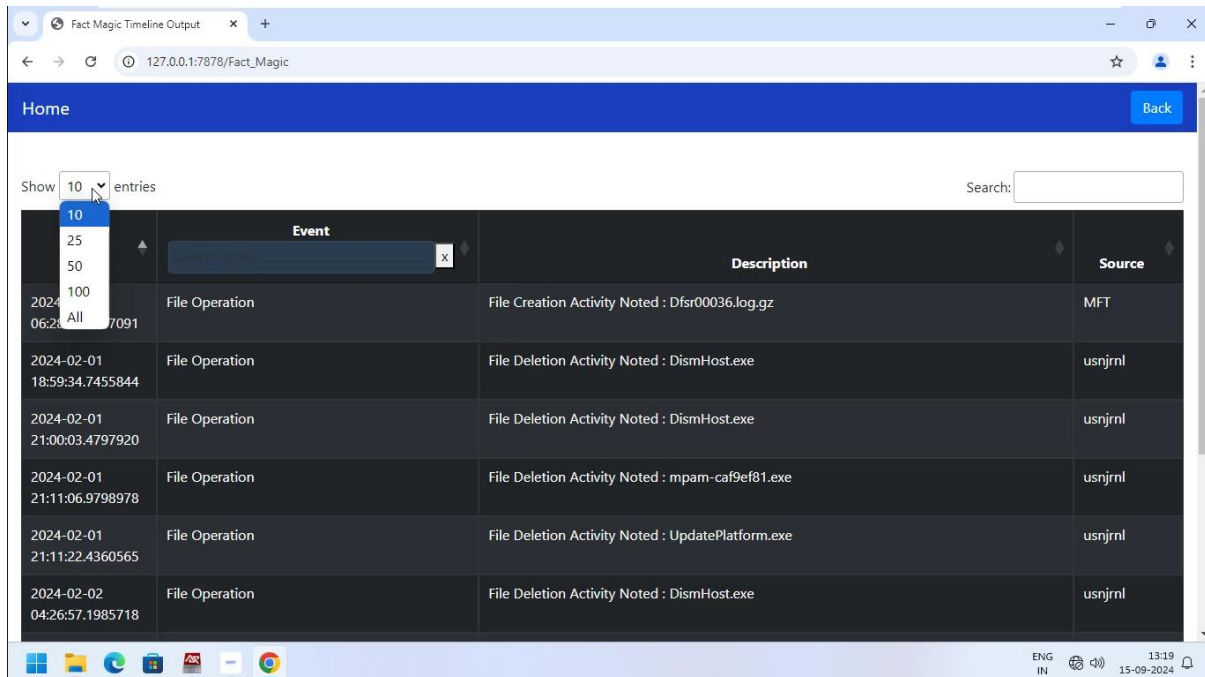
13. Give Start Date and End Date based on your investigation requirements.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1:7878/Fact\_Magic\_Date". The page has a blue header with "Home" and a "Back" button. Below the header, there are two date input fields. The first field contains "02/01/2024" and the second field contains "02/27/2024". A blue "Submit" button is located below the date fields.

*Note: use MM/DD/YYYY format.*

14. Once you hit submit button it will take some time to analyse data and it will provide you crisp timeline. You will able to filter out table based on Event Filter and additionally you can do searching also.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1:7878/Fact\_Magic". The page has a blue header with "Home" and a "Back" button. Below the header, there is a "Show 10 entries" dropdown menu and a "Search:" input field. The main content is a table with the following columns: "Event", "Description", and "Source". The table contains several rows of data, including file operations and deletions.

Event	Description	Source
File Operation	File Creation Activity Noted : Dfsr00036.log.gz	MFT
File Operation	File Deletion Activity Noted : DismHost.exe	usnjrnl
File Operation	File Deletion Activity Noted : DismHost.exe	usnjrnl
File Operation	File Deletion Activity Noted : mpam-caf9ef81.exe	usnjrnl
File Operation	File Deletion Activity Noted : UpdatePlatform.exe	usnjrnl
File Operation	File Deletion Activity Noted : DismHost.exe	usnjrnl

Fact Magic Timeline Output

127.0.0.1:7878/Fact\_Magic

Home

Back

Show All entries

Search:

Time	Event	Description	Source
2024-02-01 06:28:43.7297091	Account Management	File Creation Activity Noted : Dfsr00036.log.gz	MFT
2024-02-01 18:59:34.7455844	Program Installation/Uninstallation	File Deletion Activity Noted : DismHost.exe	usnjrnl
2024-02-01 21:00:03.4797920	File Operation	File Deletion Activity Noted : DismHost.exe	usnjrnl
2024-02-01 21:11:06.9798978	File Operation	File Deletion Activity Noted : mpam-caf9ef81.exe	usnjrnl
2024-02-01 21:11:22.4360565	File Operation	File Deletion Activity Noted : UpdatePlatform.exe	usnjrnl
2024-02-02 04:26:57.1985718	File Operation	File Deletion Activity Noted : DismHost.exe	usnjrnl

ENG IN

13:19

15-09-2024

Fact Magic Timeline Output

127.0.0.1:7878/Fact\_Magic

Home

Back

Show All entries

Search:

Time	Event	Description	Source
2024-02-05 23:02:00.9700560	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-1057484085-1795310446-2370380301-2611 TargetUserName: admin SubjectUserSid: S-1-5-21-1057484085-1795310446-2370380301-500 SubjectUserName: Administrator	Security.evtx
2024-02-05 23:42:18.6874562	Program Installation/Uninstallation	Event ID: 11707. Installation Operation Completed Successfully. Program: Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31332	Application.evtx
2024-02-05 23:42:20.8808189	Program Installation/Uninstallation	Event ID: 11707. Installation Operation Completed Successfully. Program: Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31332	Application.evtx

Showing 1 to 3 of 3 entries (filtered from 177 total entries)

Previous 1 Next

ENG IN

13:20

15-09-2024

Fact Magic Timeline Output

127.0.0.1:7878/Fact\_Magic

Home

Back

Show 

All

 entries

Search: 

sys

Time	Event	Description	Source
	<div><div>&gt; Account Management</div><div>&gt; File Operation</div><div>&gt; Program Installation/Uninstallation</div><div>&gt; RDP - Failed Logon</div></div>		
2024-02-05 23:14:25.9914284	File Operation	File Deletion Activity Noted : Temp1_SysinternalsSuite.zip	usnjrnl

Showing 1 to 1 of 1 entries (filtered from 177 total entries)

Previous

1

Next

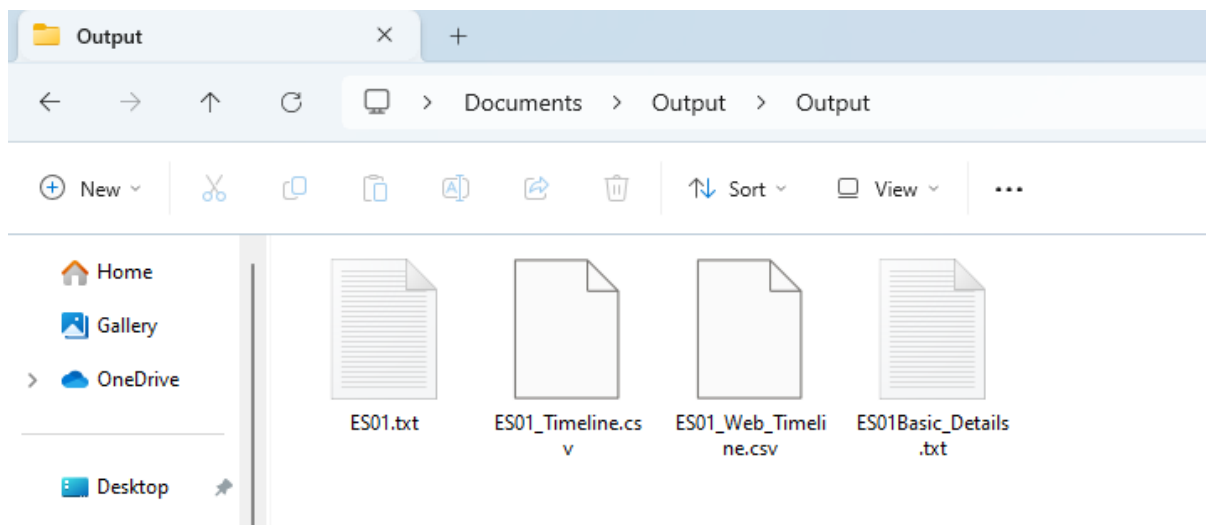
ENG IN 13:20 15-09-2024

15. Timeline will have following 4 fields:

- a. Time: Date and Time of the Event
- b. Event: Category of the Event
- c. Description: Detailed Information about the Event
- d. Source: Origin of the Event Details

16. Additionally check the output folder and inside that you need to navigate to Output folder and you will see the 4 files.

- a. Text file: will contain Basic Details
- b. CVS file: will contains the output of timeline.



## Detective's Handbook: Troubleshooting Common Dilemmas

*Find future updates based on community feedback under this section.*

**In FACT.exe terminal it says Collection Ended but when clicked on Basic Details in Web Browser it gives error.**

```
Processing chunk 2,471 of 4800 % complete: 51.48% Records found: 2,55,310
* Serving Flask app 'app'
* Debug mode: off
Collection Started
Please Wait 600 seconds, Collection is going on
Please Wait - 300 Seconds, Collection is going on
Please Wait - 180 Seconds, Collection is going on
Please Wait - 30 Seconds, Collection is going on
Collection End
```

Certain times you will see FACT.exe Terminal Screen will display “Collection End” but in top you can see “Processing chunk” line which indicates that still processing is going.

As soon as processing completes you will see something like “Total Execution Time”. Which indicates processing is completed.

```
Total execution time: 1,134.8545 seconds
* Serving Flask app 'app'
* Debug mode: off
Collection Started
Please Wait 600 seconds, Collection is going on
Please Wait - 300 Seconds, Collection is going on
Please Wait - 180 Seconds, Collection is going on
Please Wait - 30 Seconds, Collection is going on
Collection End
```



## SOS: Emergency Contacts for the FACT

In case of any issues related to the tool, please refer to the following contacts for assistance:

**Developer Contact / Technical Assistant:**

Email: [developeronvacation@gmail.com](mailto:developeronvacation@gmail.com)