FACT

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.

Table of Contents

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.

Essential Setup: Ready, Steady & Analyse with Investigative Arsenal

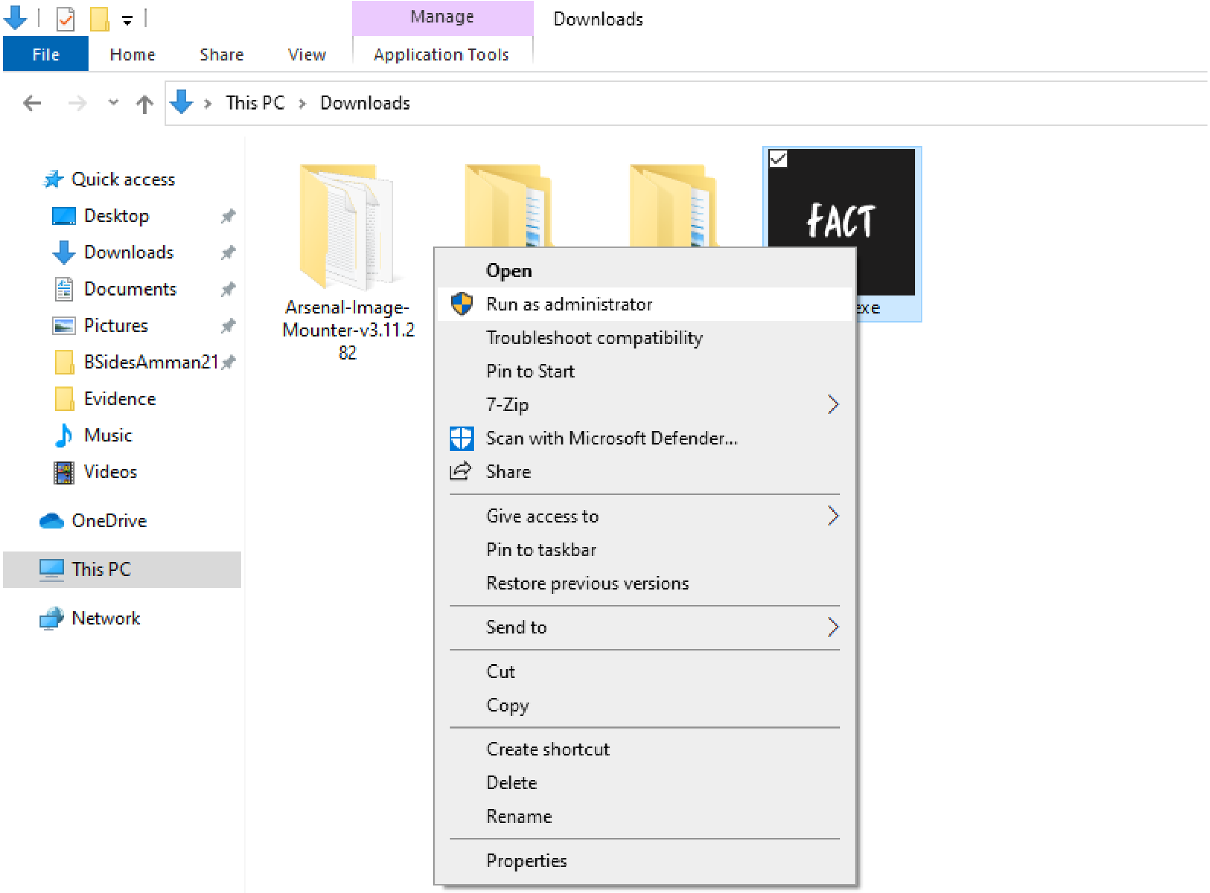
FACT requires fulfilling of the following prerequisites for successful execution.

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

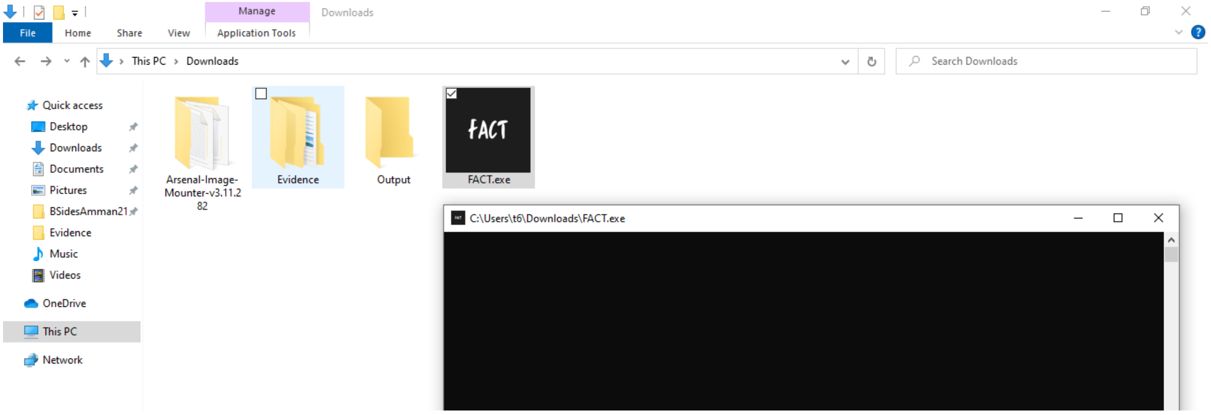
Note: Always ensure that the targeted Windows disk image is mounted using Arsenal Image Mounter for optimal performance and reliability.

Deciphering Clues

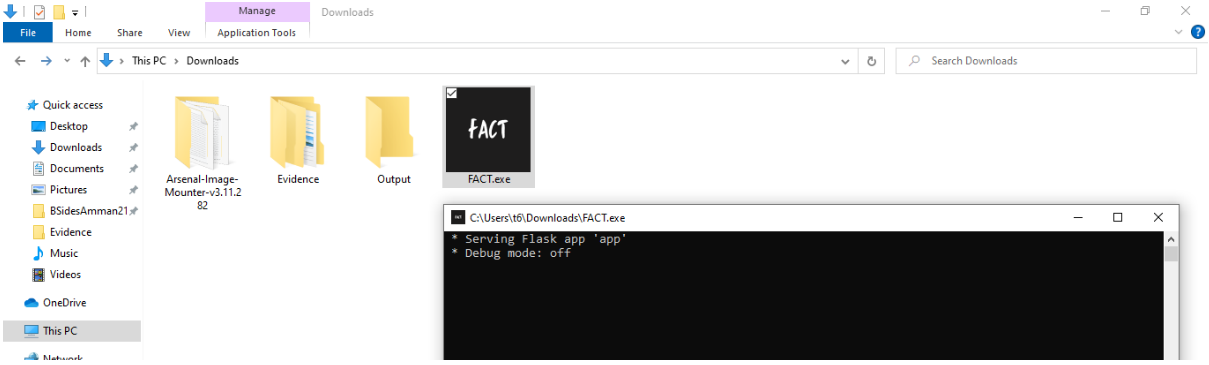
1. Run executable FACT.exe with administrative privileges.



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

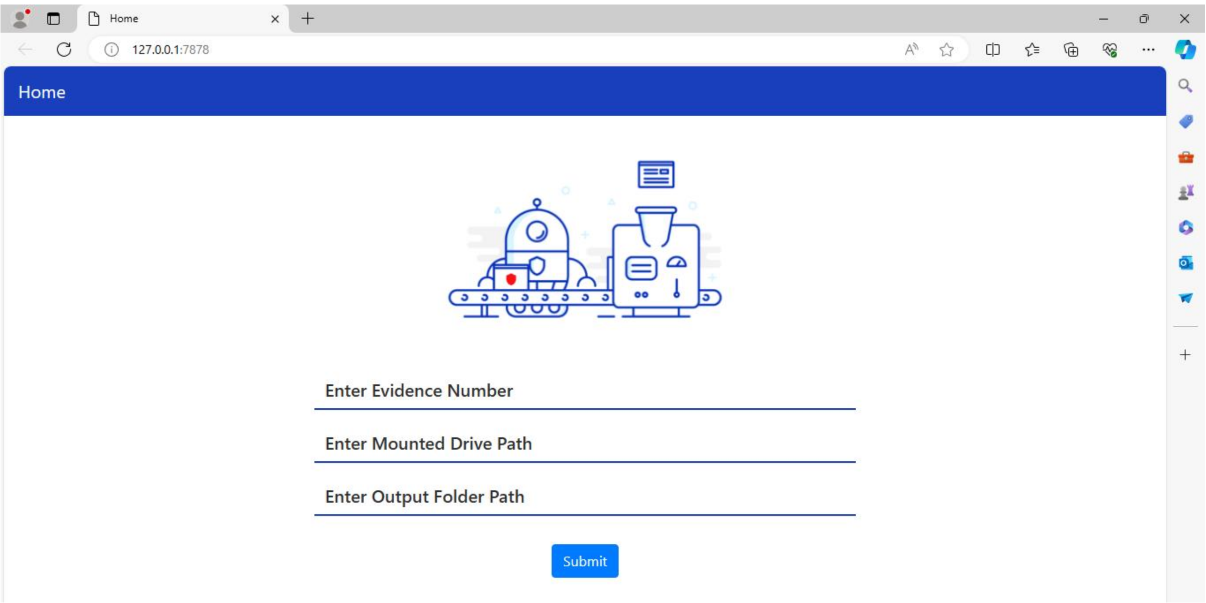


3. You will encounter the following screen during the loading process.



```
 * Serving Flask app 'app'
 * Debug mode: off
```

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



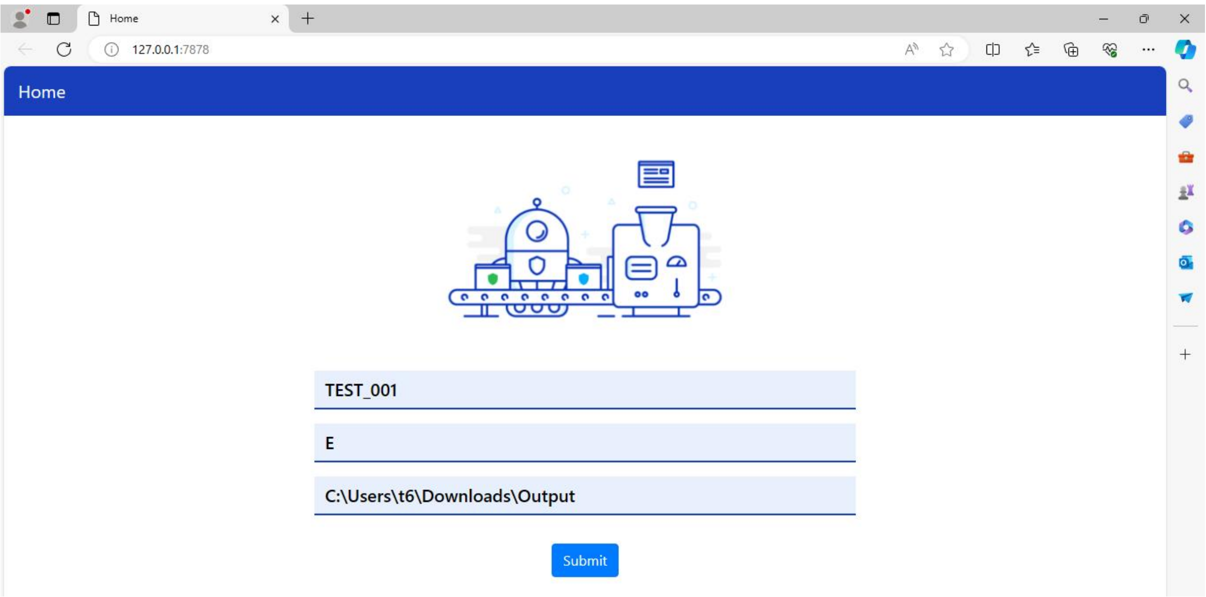
Enter Evidence Number

Enter Mounted Drive Path

Enter Output Folder Path

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

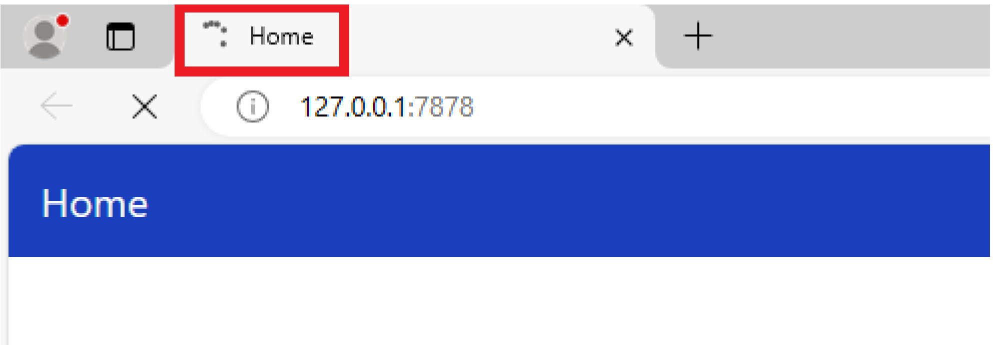


TEST_001

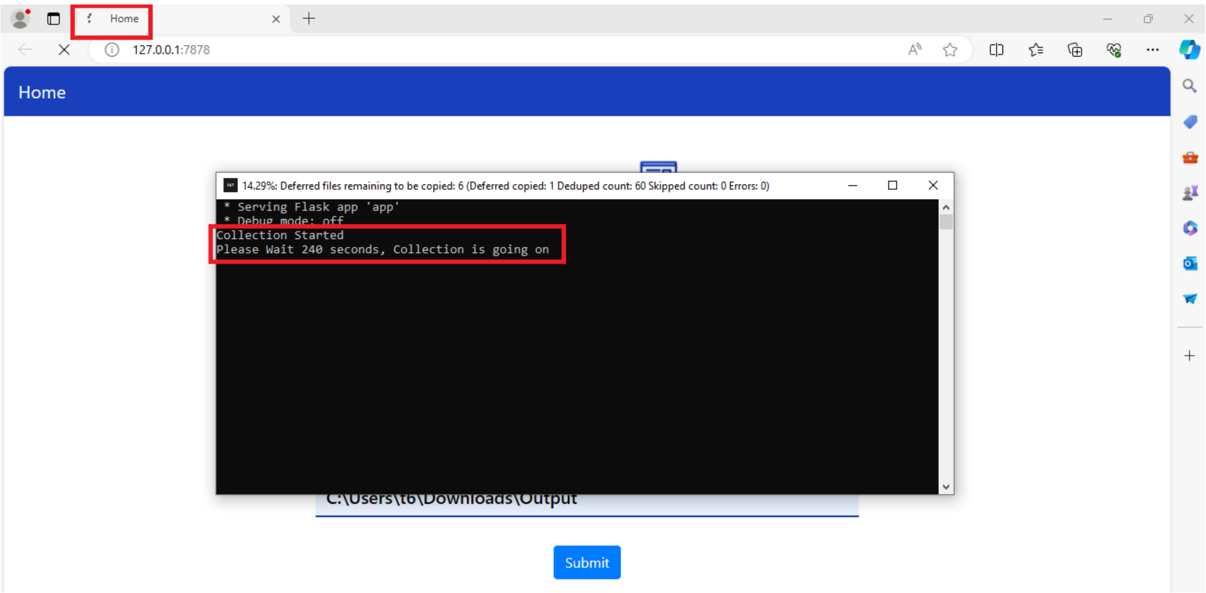
E

C:\Users\t6\Downloads\Output

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.

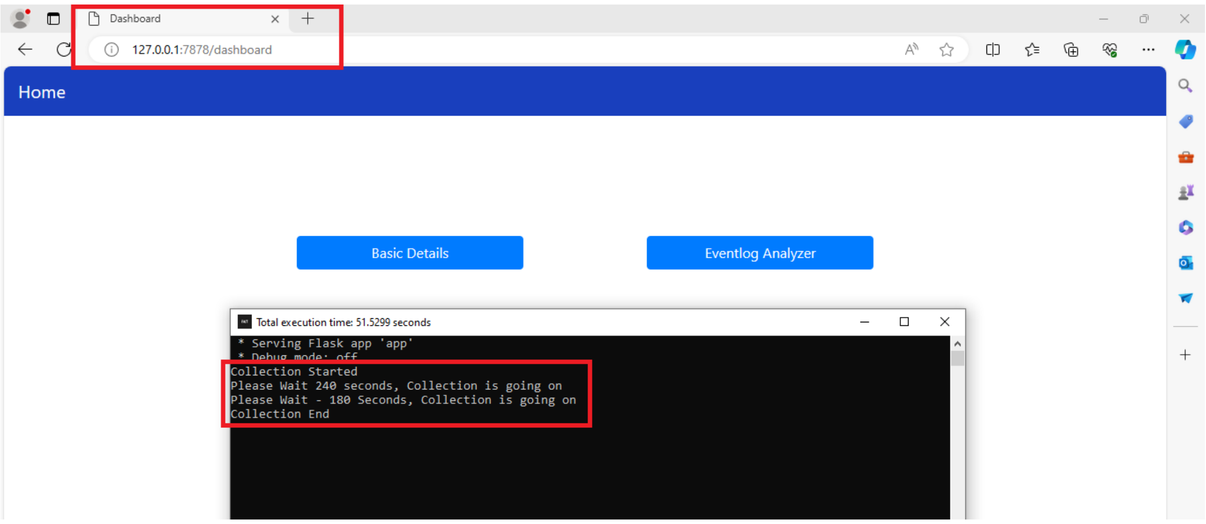


14.29%: Deferred files remaining to be copied: 6 (Deferred copied: 1 Deduped count: 60 Skipped count: 0 Errors: 0)

```
 * Serving Flask app 'app'
 * Debug mode: off
Collection Started
Please Wait 240 seconds, Collection is going on
```

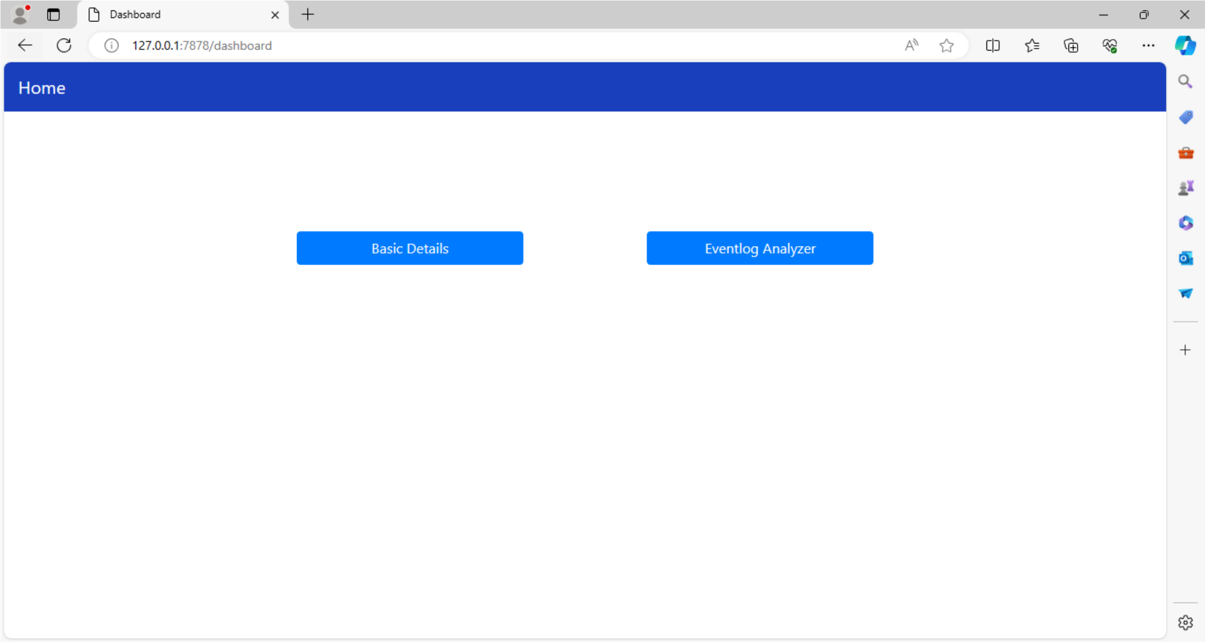
C:\Users\t6\Downloads\Output

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

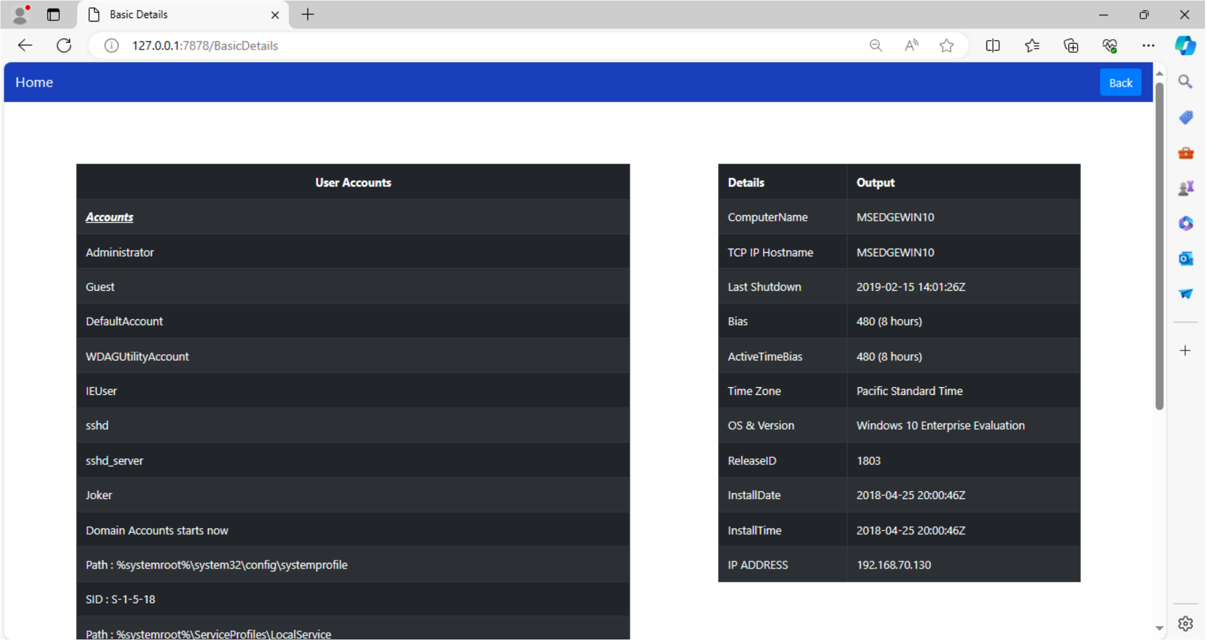


Total execution time: 51.5299 seconds

```
 * Serving Flask app 'app'
 * Debug mode: off
Collection Started
Please Wait 240 seconds, Collection is going on
Please Wait - 180 Seconds, Collection is going on
Collection End
```



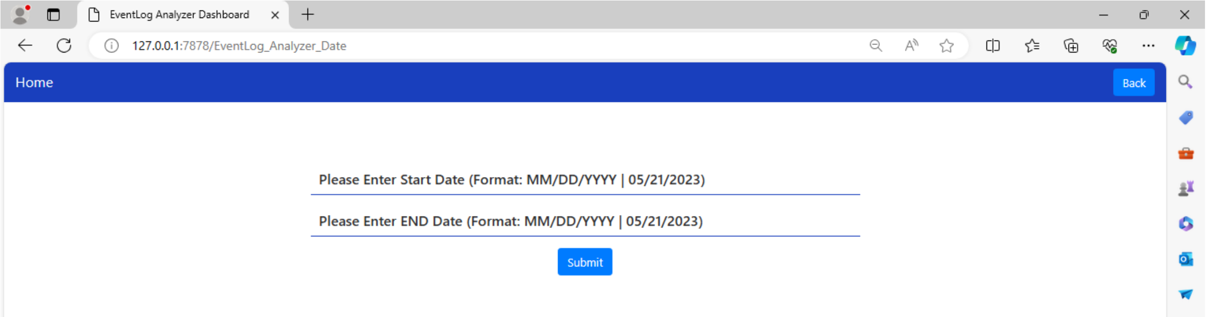
11. Now Click on Basic Details to uncover the basic information from the mounted evidence.



User Accounts
Accounts
Administrator
Guest
DefaultAccount
WDAGUtilityAccount
IEUser
sshd
sshd_server
Joker
Domain Accounts starts now
Path : %systemroot%\system32\config\systemprofile
SID : S-1-5-18
Path : %systemroot%\ServiceProfiles\LocalService

Details	Output
ComputerName	MSEDGEWIN10
TCP IP Hostname	MSEDGEWIN10
Last Shutdown	2019-02-15 14:01:26Z
Bias	480 (8 hours)
ActiveTimeBias	480 (8 hours)
Time Zone	Pacific Standard Time
OS & Version	Windows 10 Enterprise Evaluation
ReleaseID	1803
InstallDate	2018-04-25 20:00:46Z
InstallTime	2018-04-25 20:00:46Z
IP ADDRESS	192.168.70.130

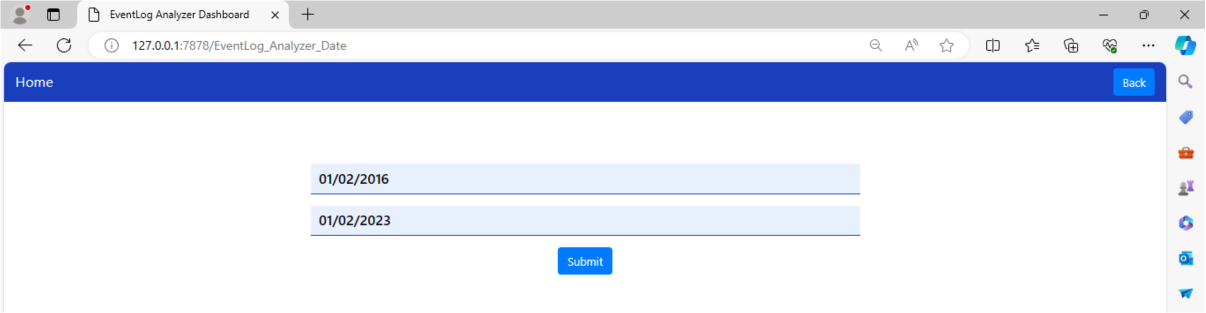
12. Further, from the dashboard click on “Eventlog Analyzer” and you will be redirected to below screen.


EventLog Analyzer Dashboard
127.0.0.1:7878/EventLog_Analyzer_Date
Home
Back
Submit

Please Enter Start Date (Format: MM/DD/YYYY | 05/21/2023)

Please Enter END Date (Format: MM/DD/YYYY | 05/21/2023)

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

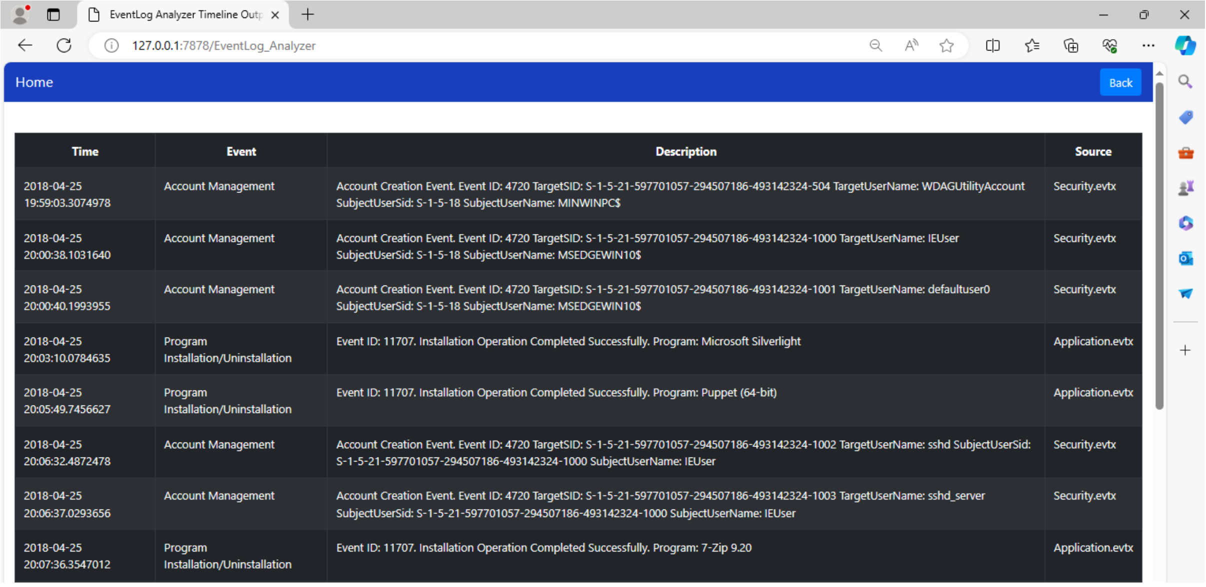

EventLog Analyzer Dashboard
127.0.0.1:7878/EventLog_Analyzer_Date
Home
Back
Submit

01/02/2016

01/02/2023

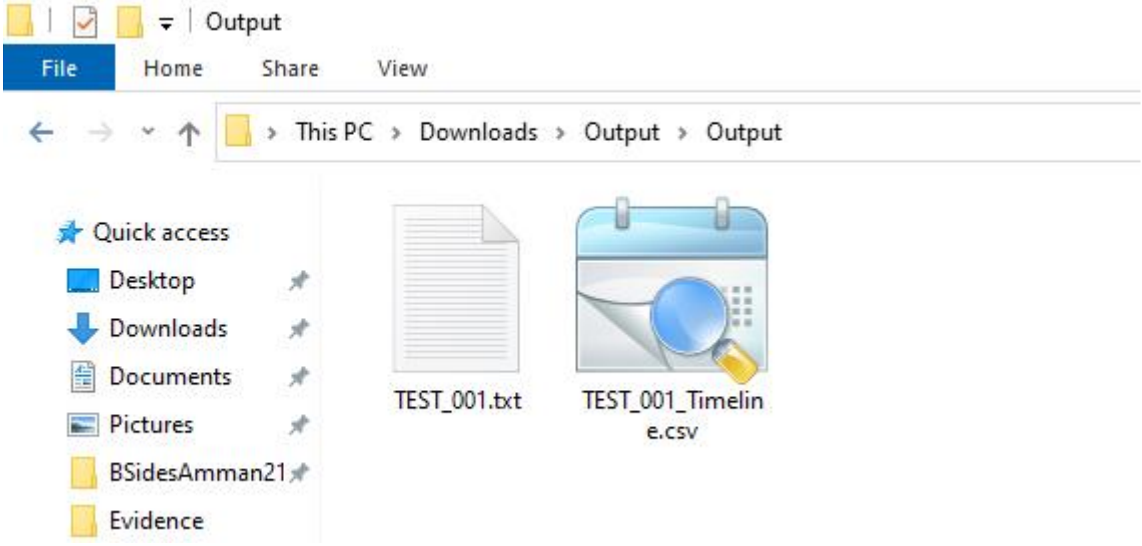
Note: use MM/DD/YYYY format.

14. Once you hit submit button it will take some time to analyse event logs and it will provide you crisp timeline.


EventLog Analyzer Timeline Outp
127.0.0.1:7878/EventLog_Analyzer
Home
Back

Time	Event	Description	Source
2018-04-25 19:59:03.3074978	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-597701057-294507186-493142324-504 TargetUserName: WDAGUtilityAccount SubjectUserSid: S-1-5-18 SubjectUserName: MINWINPC$	Security.evtx
2018-04-25 20:00:38.1031640	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-597701057-294507186-493142324-1000 TargetUserName: IEUser SubjectUserSid: S-1-5-18 SubjectUserName: MSEDGEWIN10$	Security.evtx
2018-04-25 20:00:40.1993955	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-597701057-294507186-493142324-1001 TargetUserName: defaultuser0 SubjectUserSid: S-1-5-18 SubjectUserName: MSEDGEWIN10$	Security.evtx
2018-04-25 20:03:10.0784635	Program Installation/Uninstallation	Event ID: 11707. Installation Operation Completed Successfully. Program: Microsoft Silverlight	Application.evtx
2018-04-25 20:05:49.7456627	Program Installation/Uninstallation	Event ID: 11707. Installation Operation Completed Successfully. Program: Puppet (64-bit)	Application.evtx
2018-04-25 20:06:32.4872478	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-597701057-294507186-493142324-1002 TargetUserName: sshd SubjectUserSid: S-1-5-21-597701057-294507186-493142324-1000 SubjectUserName: IEUser	Security.evtx
2018-04-25 20:06:37.0293656	Account Management	Account Creation Event. Event ID: 4720 TargetSID: S-1-5-21-597701057-294507186-493142324-1003 TargetUserName: sshd_server SubjectUserSid: S-1-5-21-597701057-294507186-493142324-1000 SubjectUserName: IEUser	Security.evtx
2018-04-25 20:07:36.3547012	Program Installation/Uninstallation	Event ID: 11707. Installation Operation Completed Successfully. Program: 7-Zip 9.20	Application.evtx

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 2 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.

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