Title: Install cyber triage and collect the given system report.Analyse your data accordingly

Objective:

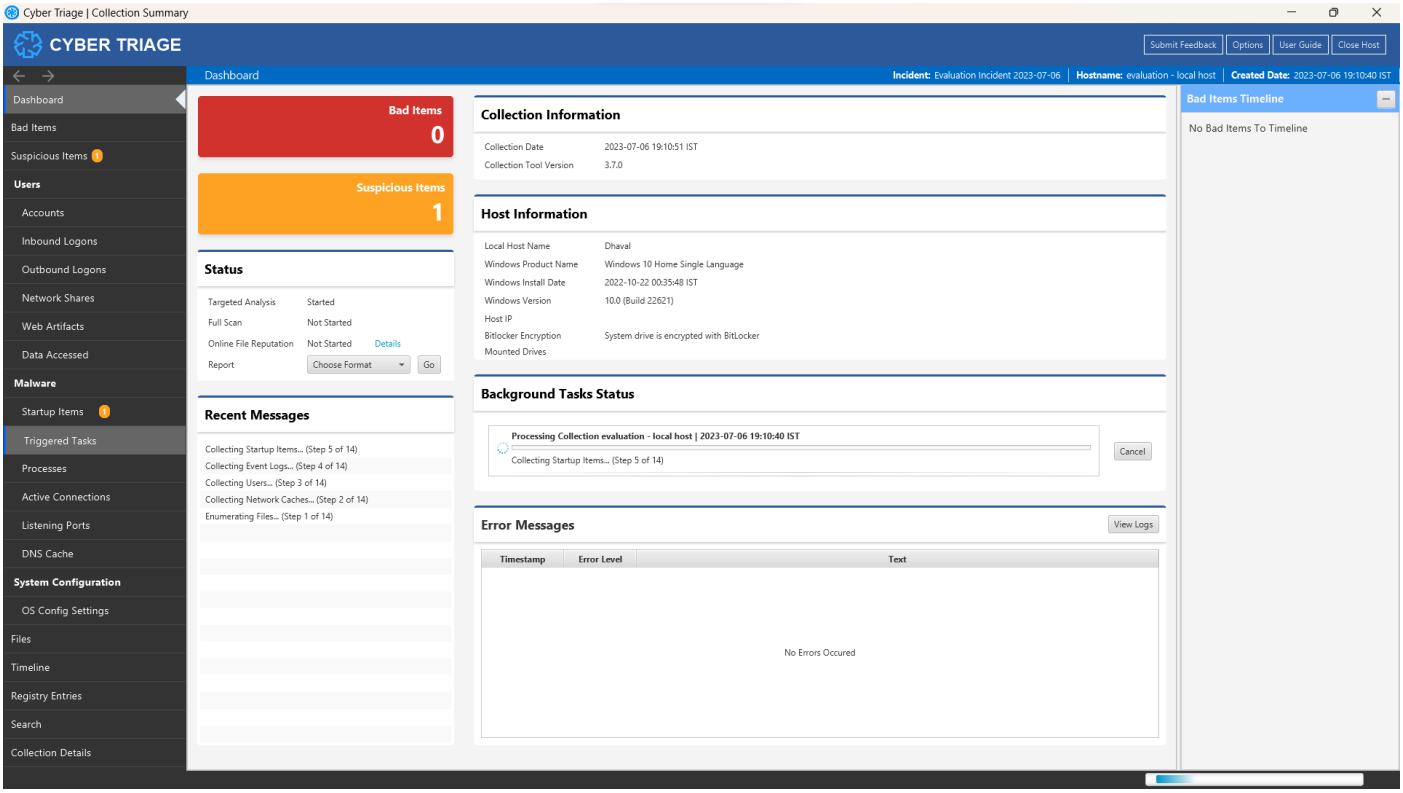
The objective of this experiment is to install Cyber Triage, a digital forensic tool, and collect a system report for analysis purposes.

Requirements:

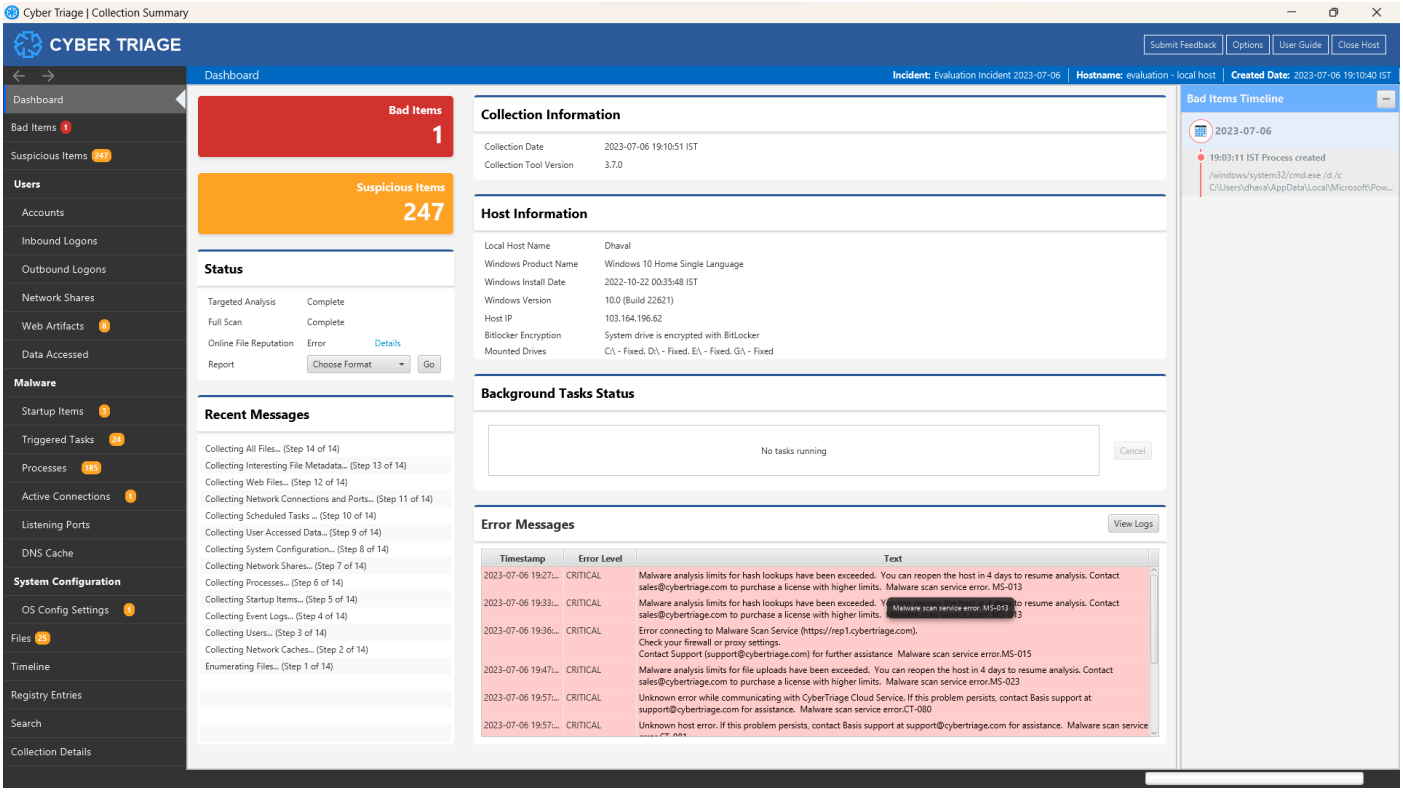
- Cyber Triage system requirements
- Internet connectivity
- Cyber Triage installation package

Procedure/Experiment Steps:

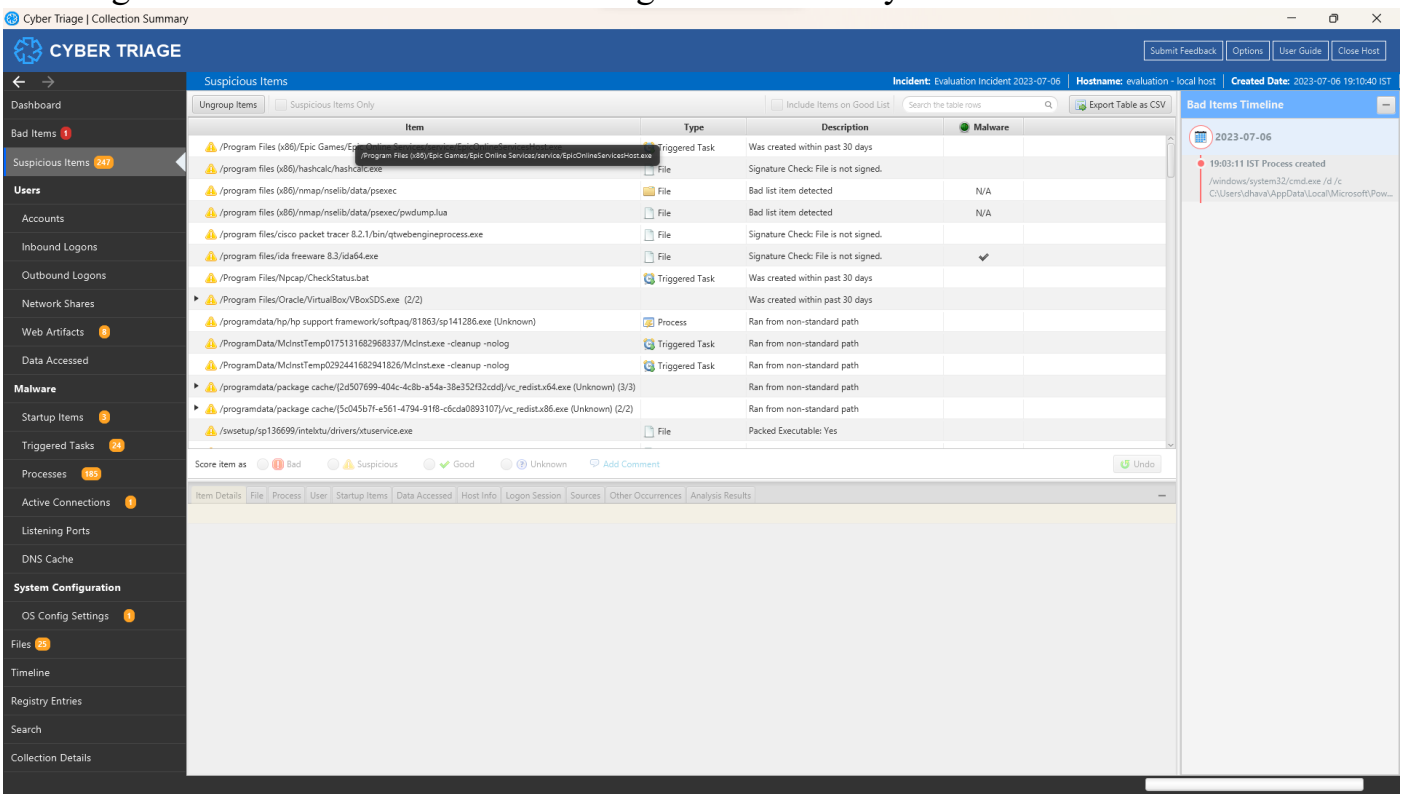
1. Download Cyber Triage: Visit the official Cyber Triage website and download the appropriate installation package for your operating system.
2. Install Cyber Triage: Follow the provided instructions to install Cyber Triage on your computer.
3. Launch Cyber Triage: After installation, launch Cyber Triage from the installed location or desktop shortcut.



4. Configure Data Collection: Set up Cyber Triage to collect the system report by selecting the appropriate options or modules within the software.

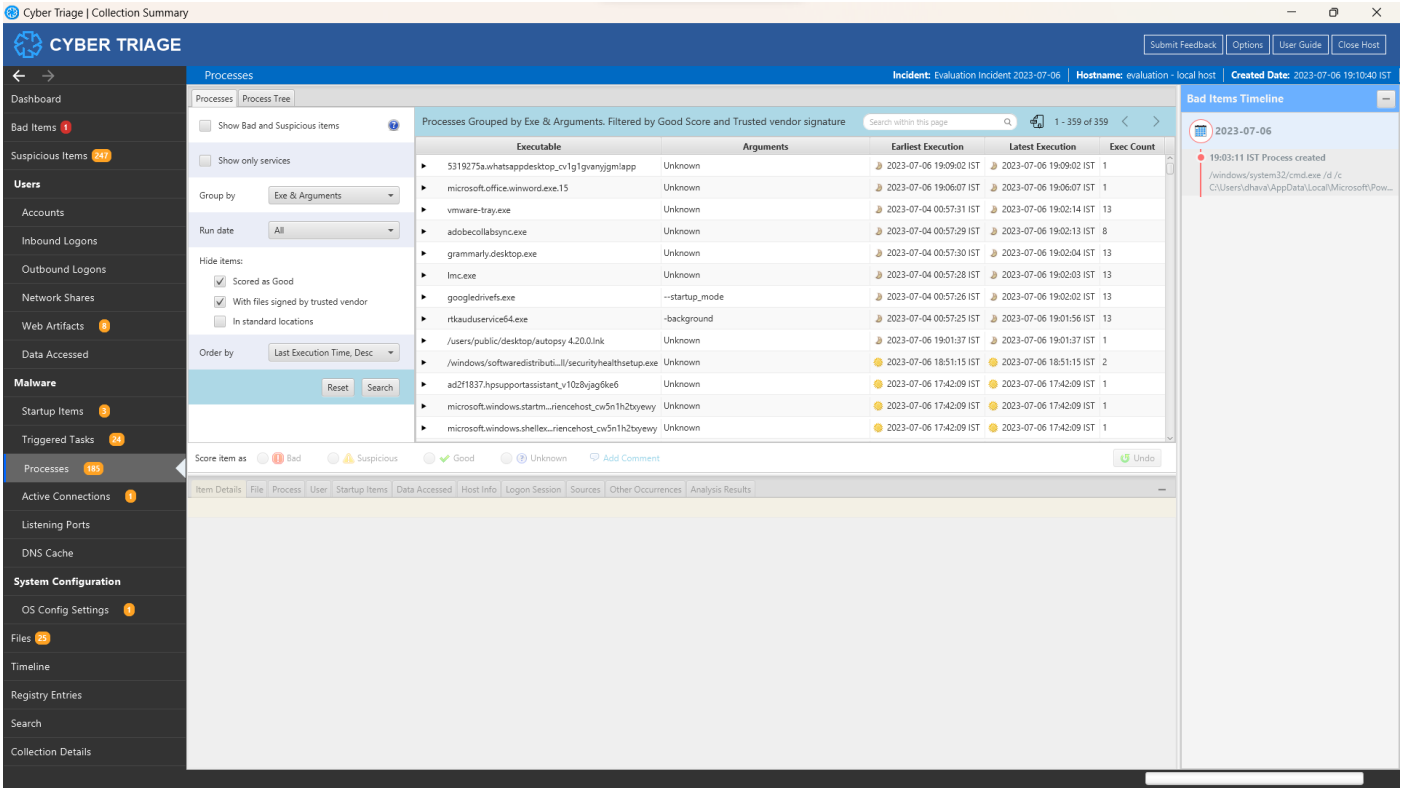


5. Initiate System Report Collection: Start the system report collection process in Cyber Triage. Allow the software to scan and gather relevant system data.



6. Wait for Data Collection to Complete: Let Cyber Triage complete the system report collection process. The duration may vary depending on the size and complexity of the system being analyzed.

7. Analyze Collected Data: Once the system report collection is finished, access the collected data within Cyber Triage for analysis.



8. Interpret System Report: Review the collected system report to extract valuable insights, identify potential security issues, and gather relevant information for further analysis.
9. Document Findings: Record the details of the analysis, including any identified issues, notable observations, or suspicious artefacts.

Result:

Using Cyber Triage, we successfully installed the software and collected a system report from the given system. After configuring the data collection settings, we initiated the collection process and allowed Cyber Triage to scan and gather the relevant system data. Once the data collection was complete, we accessed and analyzed the collected data within Cyber Triage, identifying potential security issues and extracting valuable insights. The findings and observations from the analysis were documented for further examination and action.

Conclusion:

Cyber Triage proved to be a reliable digital forensic tool for system report collection and analysis. By installing and utilizing Cyber Triage, we were able to gather comprehensive system data and gain insights into potential security issues. The software provides a valuable resource for digital forensic investigations, incident response, and proactive system monitoring.

Future Scope:

1. Deeper analysis capabilities: Utilize advanced features within Cyber Triage to conduct more in-depth analysis, such as memory forensics, timeline analysis, or file carving.
2. Integration with other forensic tools: Explore the integration of Cyber Triage with other digital forensic tools for a more comprehensive and cross-validated analysis.
3. Automation and scripting: Investigate the automation capabilities of Cyber Triage, enabling the creation of custom workflows and scripts to streamline analysis processes.

4. Threat intelligence integration: Integrate Cyber Triage with threat intelligence platforms to enhance analysis by correlating system data with known indicators of compromise.
5. Reporting and visualization: Utilize Cyber Triage's reporting and visualization features to generate comprehensive reports, graphs, and charts for easier data interpretation and communication with stakeholders.