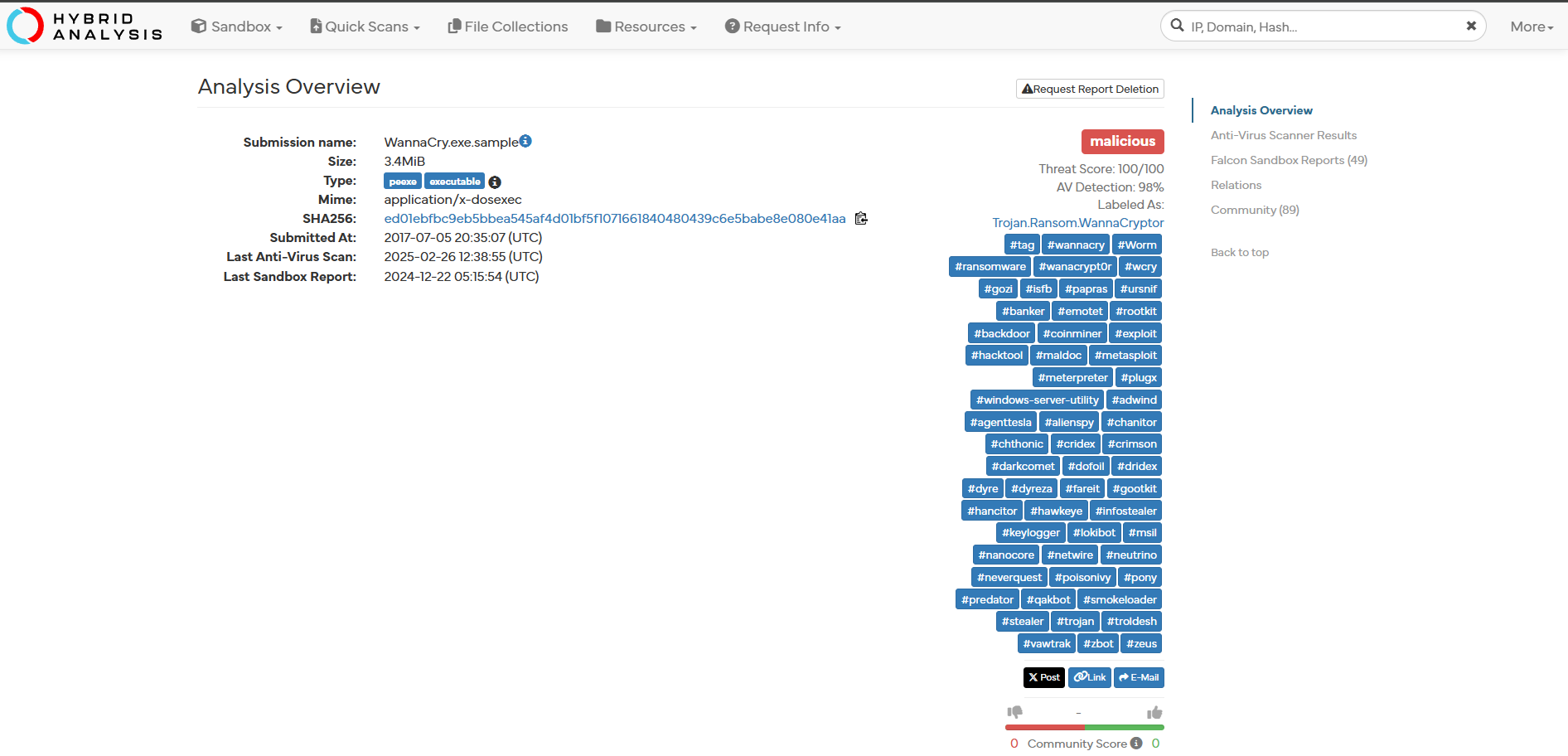
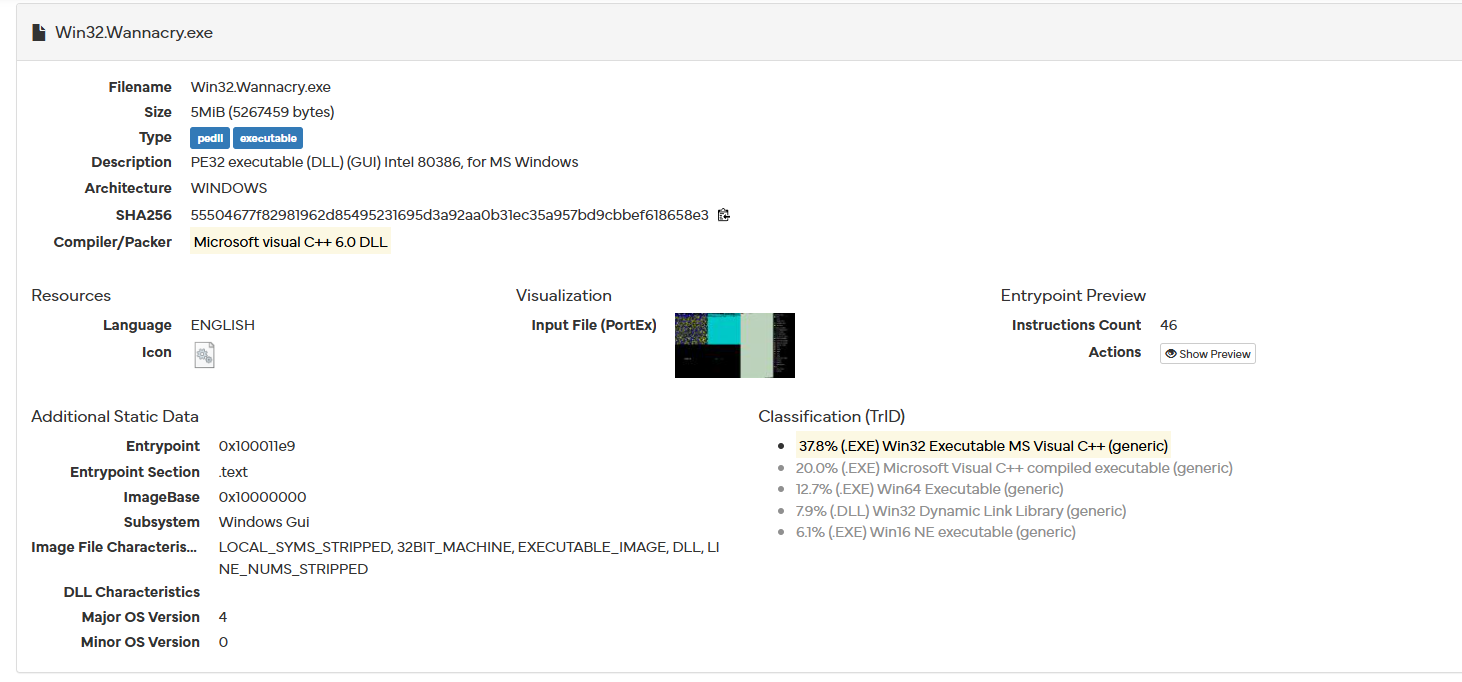
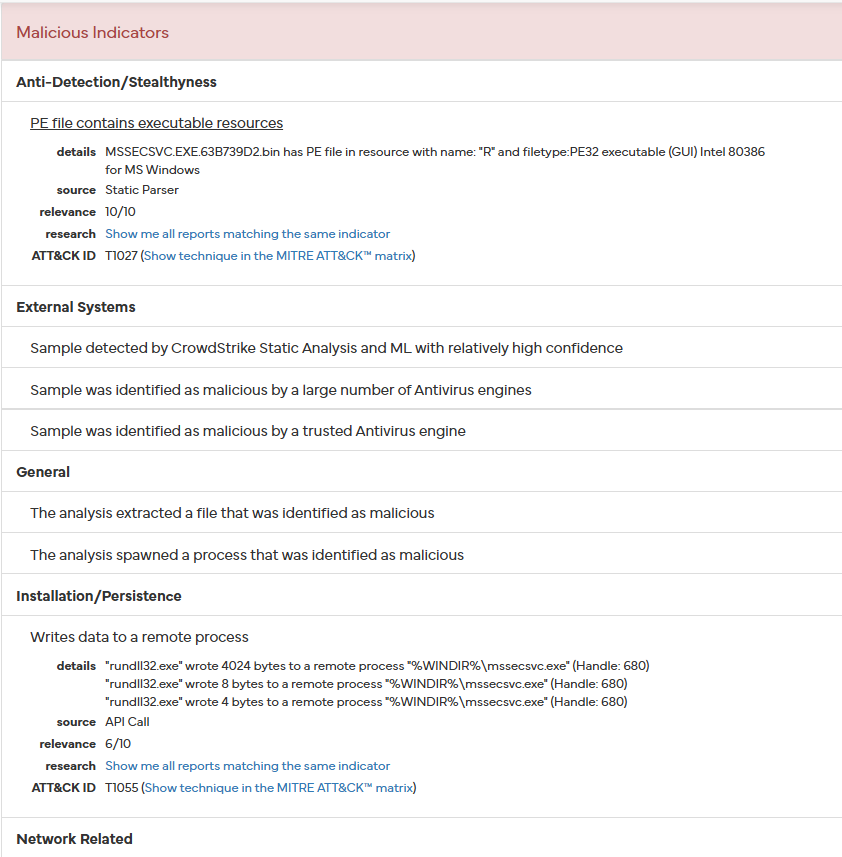
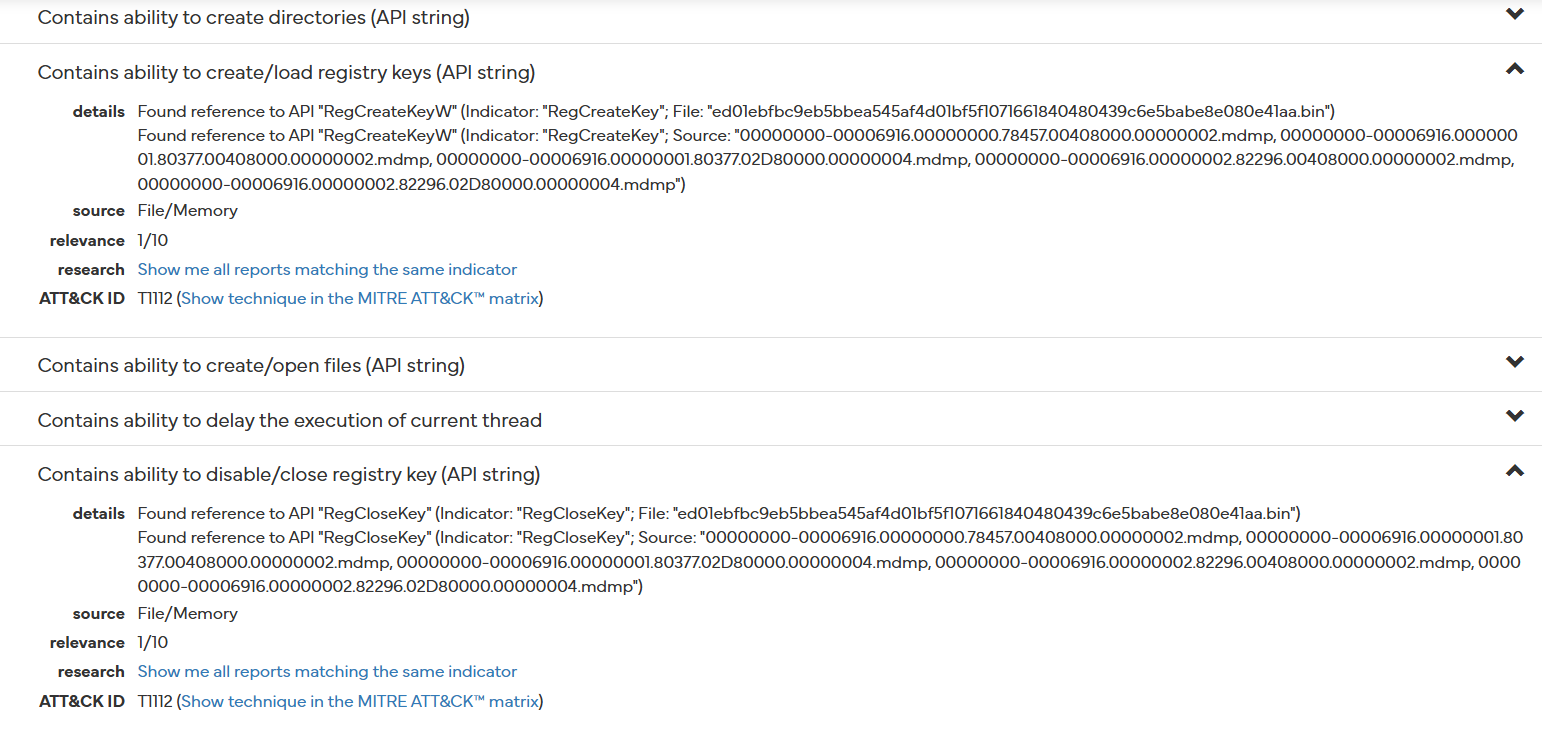
**(A)MALWARE BEHAVIOR ANALYSIS**

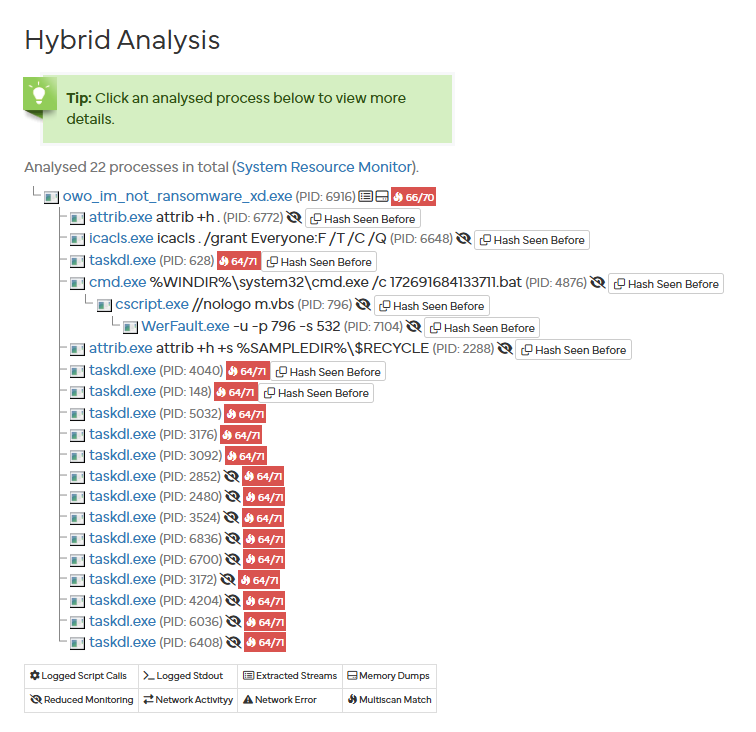
**(Using hybrid analysis)**

* **Hybrid analysis to analyze a sample malware (using test files)**
* **File details of the test file**
* **Changes occur after malware affecting the process**

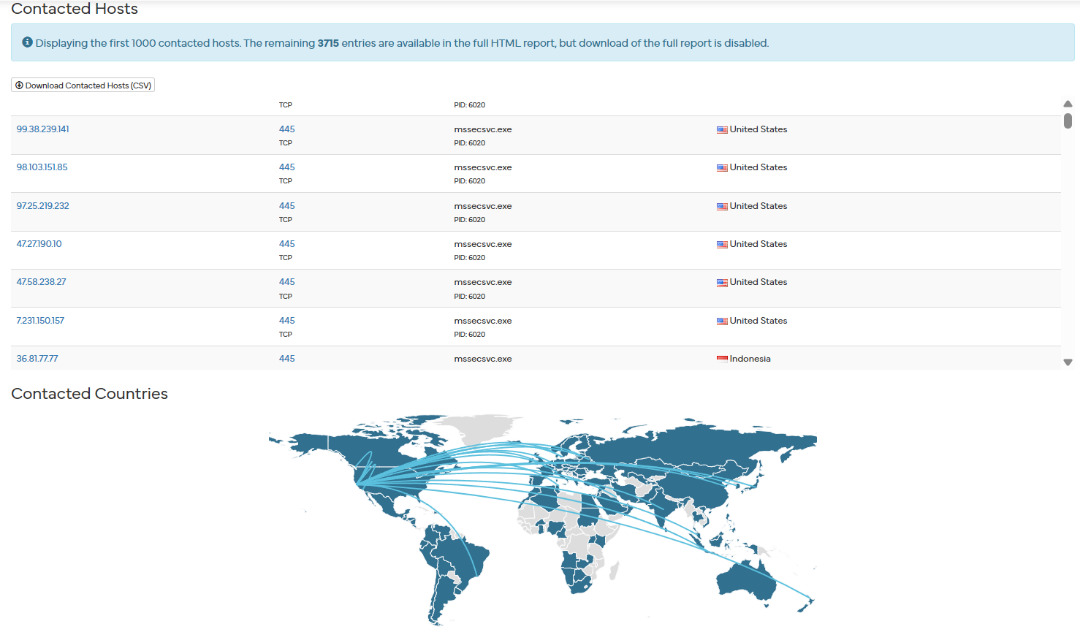
****



* **After malware affecting the process it is creating multiple process to replace test files in the system**



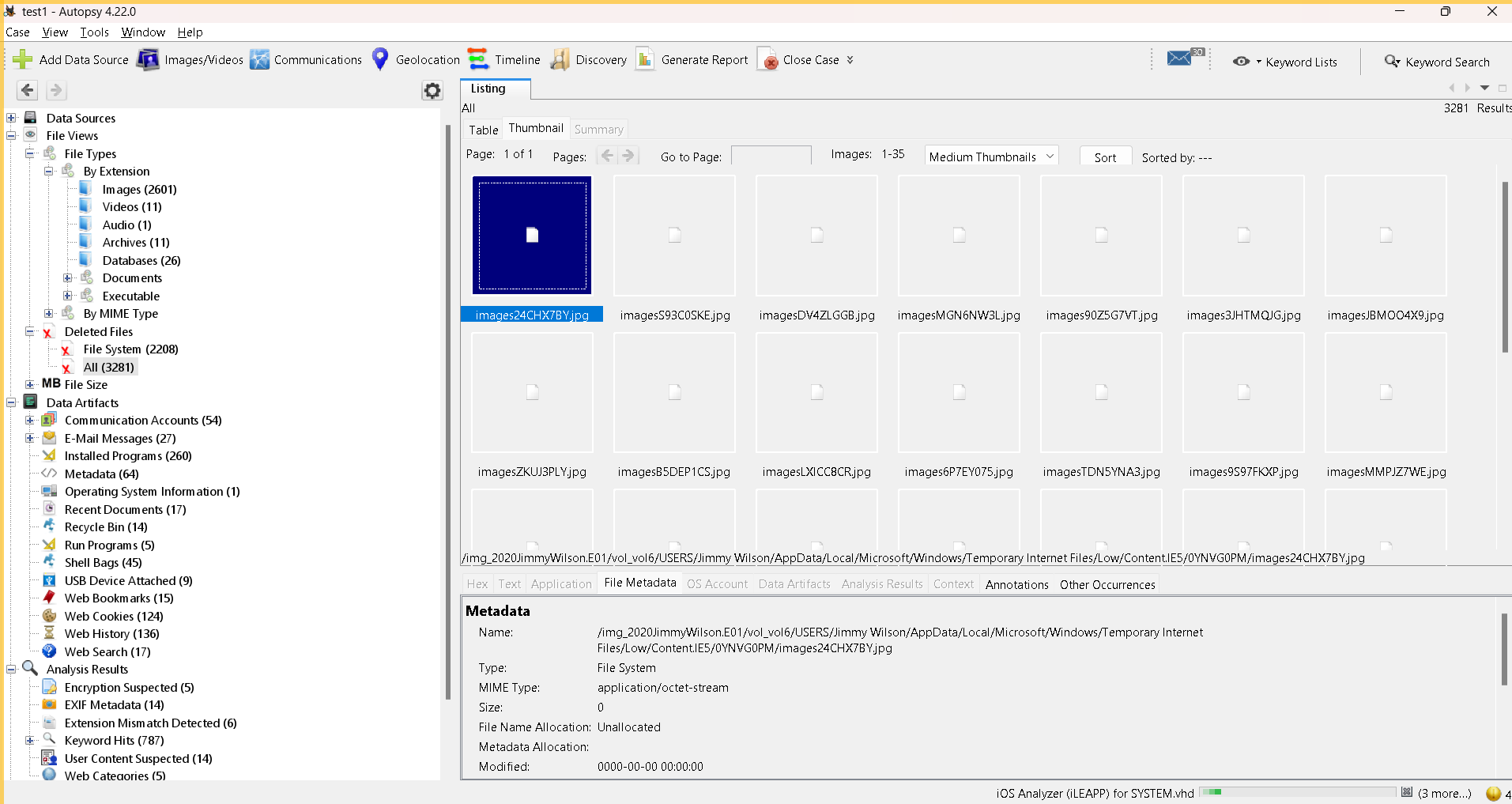
* **After running in virtual system malware tried connect and spread to other vulnerable system**



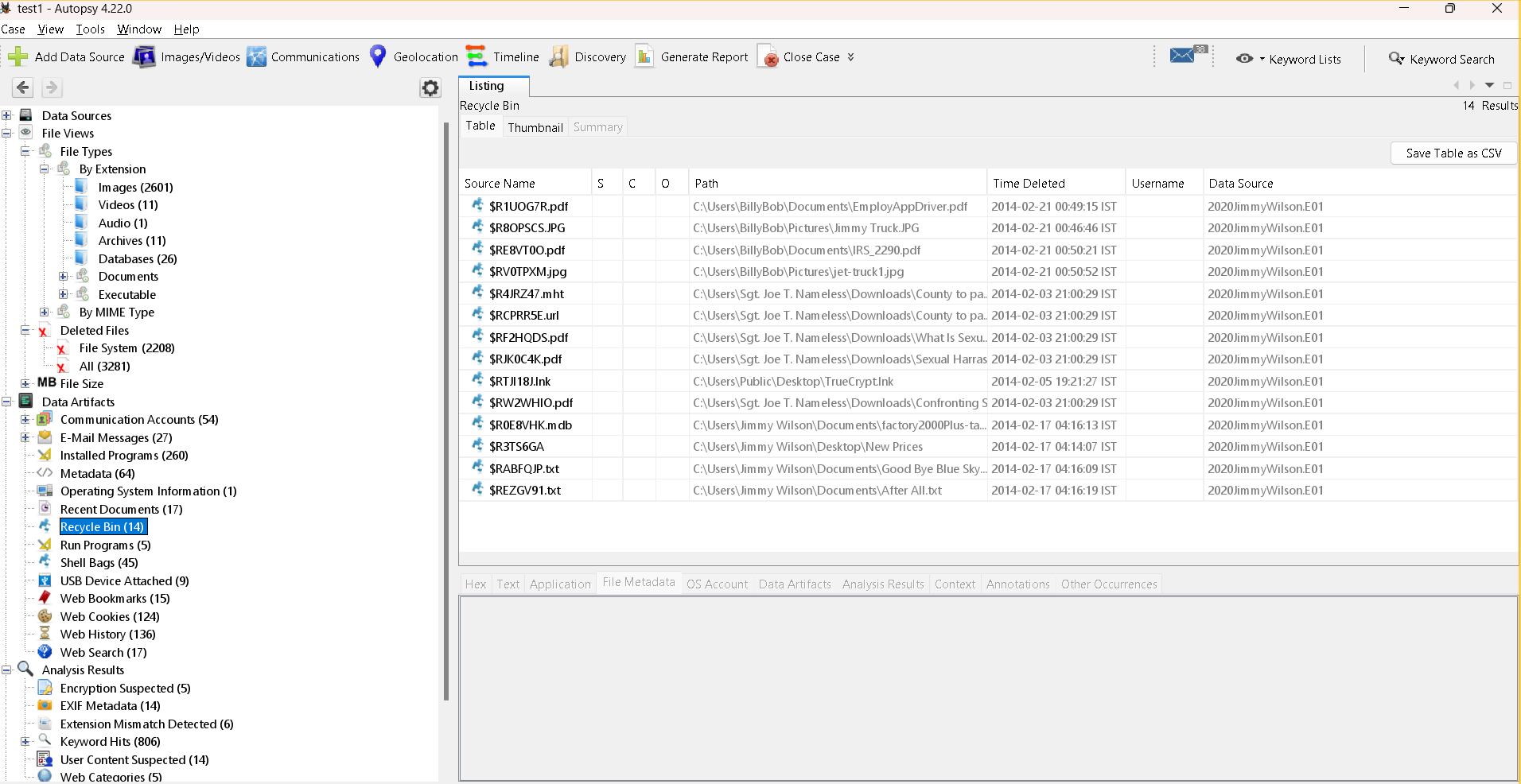
**(B)Digital Forensics Task (Using Autopsy)**

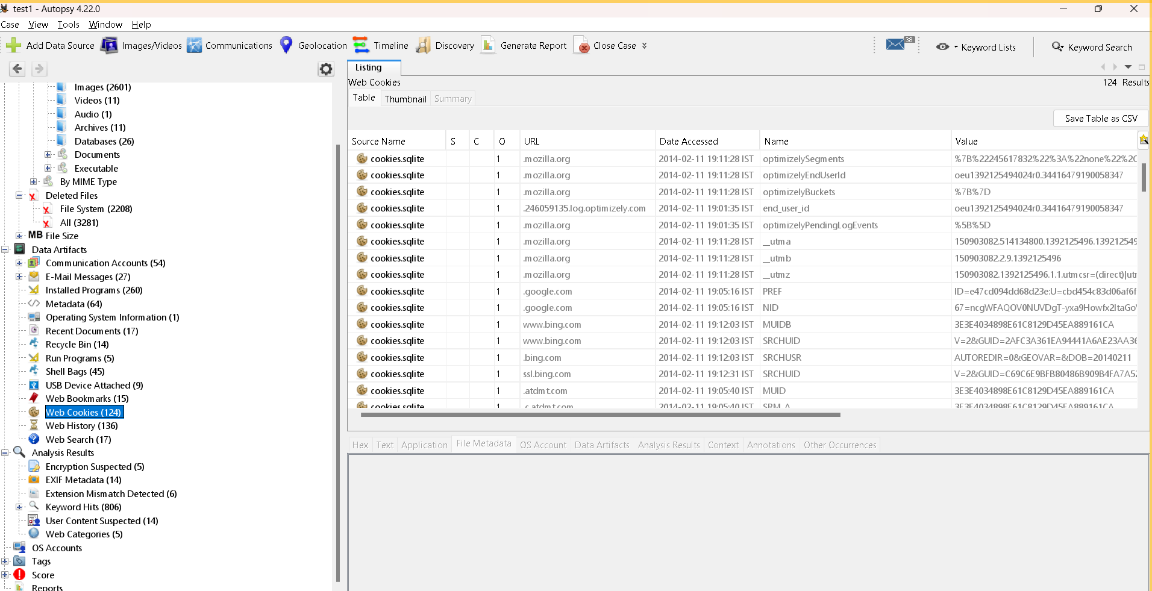
Step1. Download or exract.E01 File.

Step2. Open autopsy and select the file and its location and finish it.

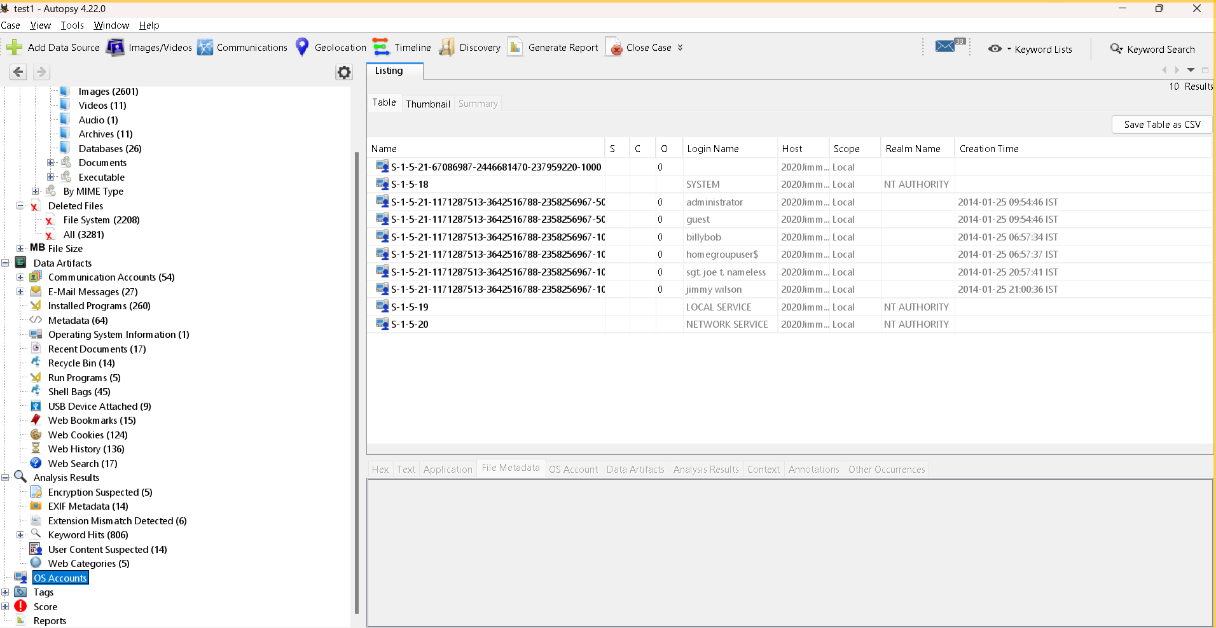
* **This interface showing details of the file. Extracting details from deleted files.**

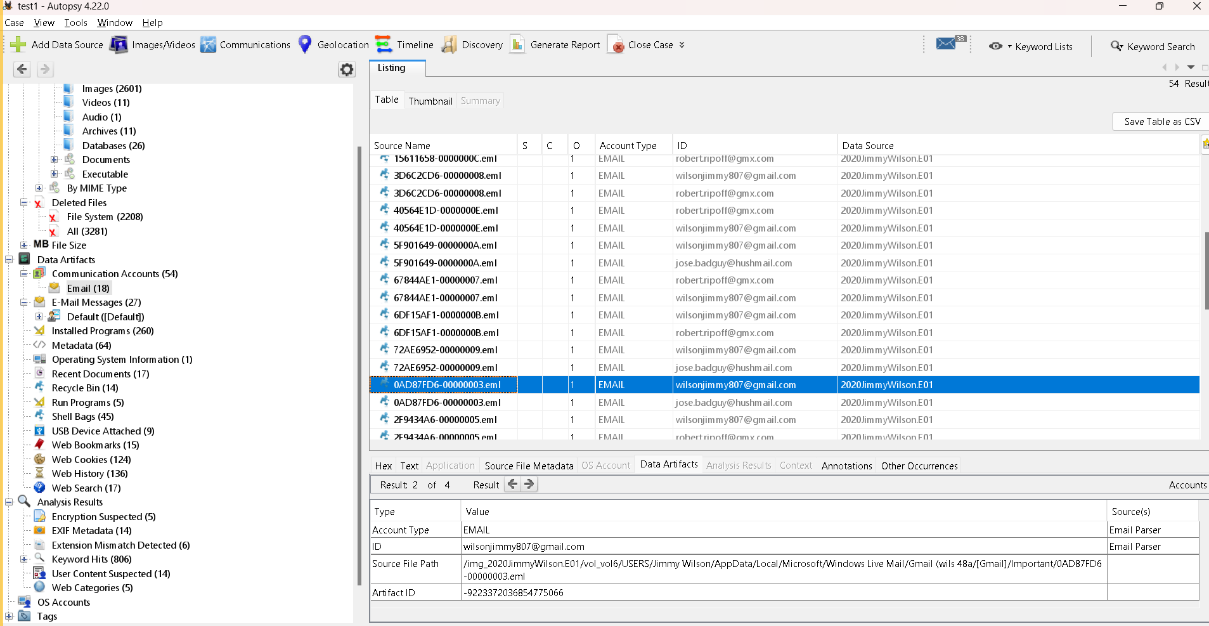


* **Extracting details from recycle bin**
* **Examining web cookies of the file**



* **Reviewing os account**



* **Checking the email details**

