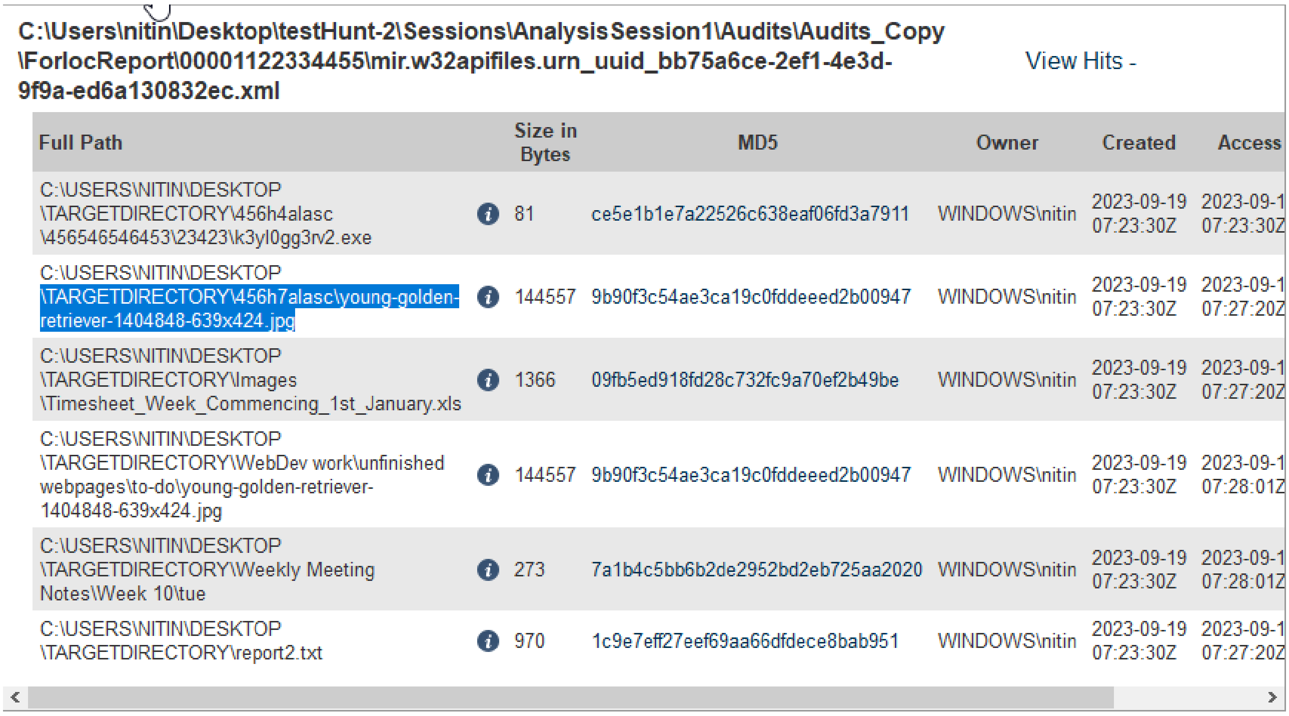
# Malware Hunting

1. How many entries are there in the IOC Report?

There are 6 entries in IOC reported.



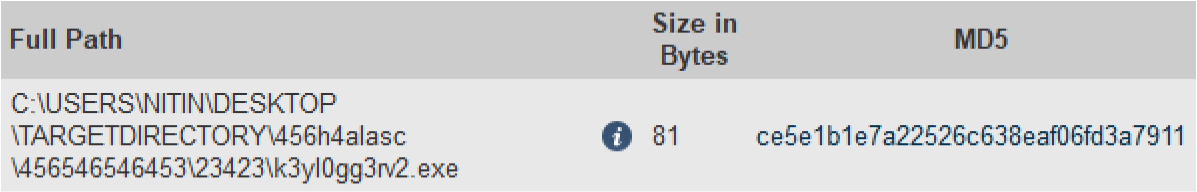
**C:\Users\nitin\Desktop\testHunt-2\Sessions\AnalysisSession1\Audits\Audits_Copy\ForlocReport\00001122334455\mir.w32apifiles.urn_uuid_bb75a6ce-2ef1-4e3d-9f9a-ed6a130832ec.xml**

View Hits -

| Full Path | | Size in Bytes | MD5 | Owner | Created | Access |
|---|---|---|---|---|---|---|
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h4alasc\456546546453\23423\k3yl0gg3rv2.exe | ⓘ | 81 | ce5e1b1e7a22526c638eaf06fd3a7911 | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:23:30Z |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 | 9b90f3c54ae3ca19c0fddeeed2b00947 | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:27:20Z |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Images\Timesheet_Week_Commencing_1st_January.xls | ⓘ | 1366 | 09fb5ed918fd28c732fc9a70ef2b49be | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:27:20Z |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\WebDev work\unfinished webpages\to-do\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 | 9b90f3c54ae3ca19c0fddeeed2b00947 | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:28:01Z |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Weekly Meeting Notes\Week 10\tue | ⓘ | 273 | 7a1b4c5bb6b2de2952bd2eb725aa2020 | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:28:01Z |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\report2.txt | ⓘ | 970 | 1c9e7eff27eef69aa66dfdece8bab951 | WINDOWS\nitin | 2023-09-19 07:23:30Z | 2023-09-1 07:27:20Z |

2. What is the file name (including extension) that has the MD5 hash of ce5e1b1e7a22526c638eaf06fd3a7911?

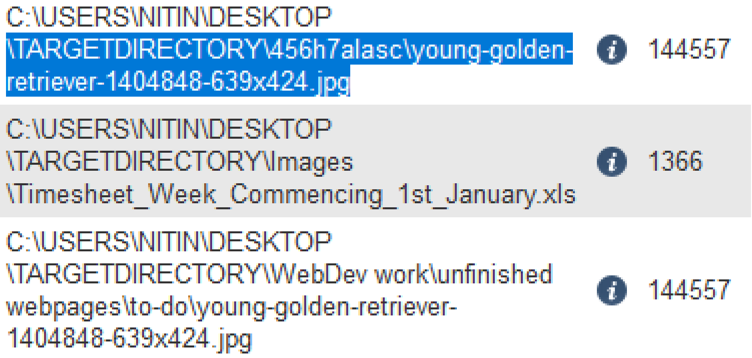
The file name (including extension) that has the MD5 hash of ce5e1b1e7a22526c638eaf06fd3a7911 is k3yl0gg3rv2.exe



| Full Path | | Size in Bytes | MD5 |
|---|---|---|---|
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h4alasc\456546546453\23423\k3yl0gg3rv2.exe | ⓘ | 81 | ce5e1b1e7a22526c638eaf06fd3a7911 |

3. What is the file path that contains the file with a size of 144557 bytes?

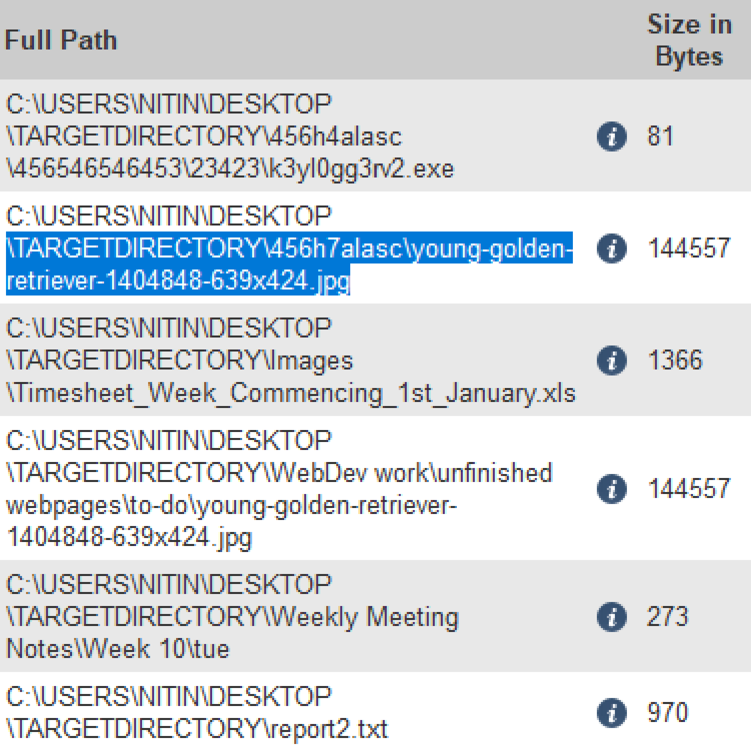
Two files contains the  file with a size of 144557 bytes. (\TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x424.jpg , \TARGETDIRECTORY\WebDev work\unfinished webpages\to-do\young-golden-retriever-1404848-639x424.jpg)



| | | |
|---|---|---|
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Images\Timesheet_Week_Commencing_1st_January.xls | ⓘ | 1366 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\WebDev work\unfinished webpages\to-do\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 |

4. Which of the following alerting file sizes are present in the IOC Report? (Multiple Choice)

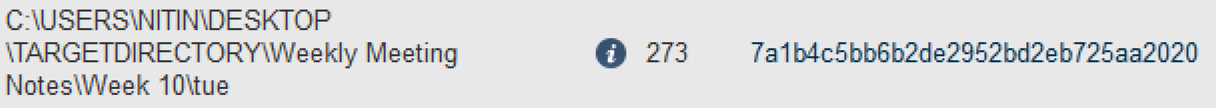
The size of the files can be seen in following picture.



| Full Path | | Size in Bytes |
|---|---|---|
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h4alasc\456546546453\23423\k3yl0gg3rv2.exe | ⓘ | 81 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Images\Timesheet_Week_Commencing_1st_January.xls | ⓘ | 1366 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\WebDev work\unfinished webpages\to-do\young-golden-retriever-1404848-639x424.jpg | ⓘ | 144557 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Weekly Meeting Notes\Week 10\tue | ⓘ | 273 |
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\report2.txt | ⓘ | 970 |

5. What is the file name that has the MD5 hash of 7a1b4c5bb6b2de2952bd2eb725aa2020?

The file name that has the MD5 hash of 7a1b4c5bb6b2de2952bd2eb725aa2020 is Tue



| | | | |
|---|---|---|---|
| C:\USERS\NITIN\DESKTOP\TARGETDIRECTORY\Weekly Meeting Notes\Week 10\tue | ⓘ | 273 | 7a1b4c5bb6b2de2952bd2eb725aa2020 |