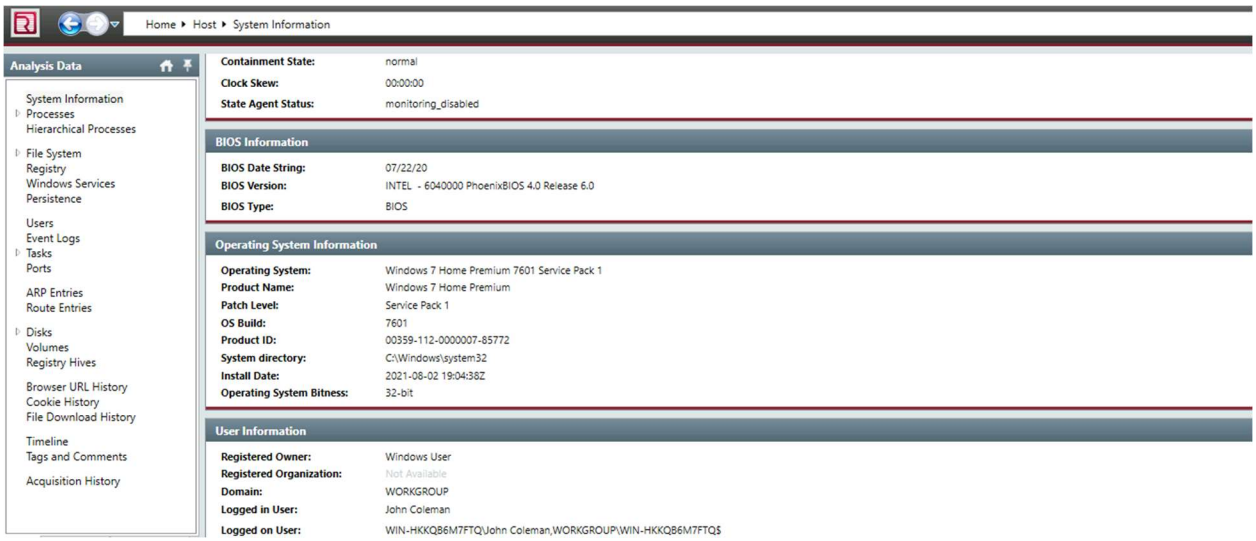
[TryHackMe | REvil Corp]

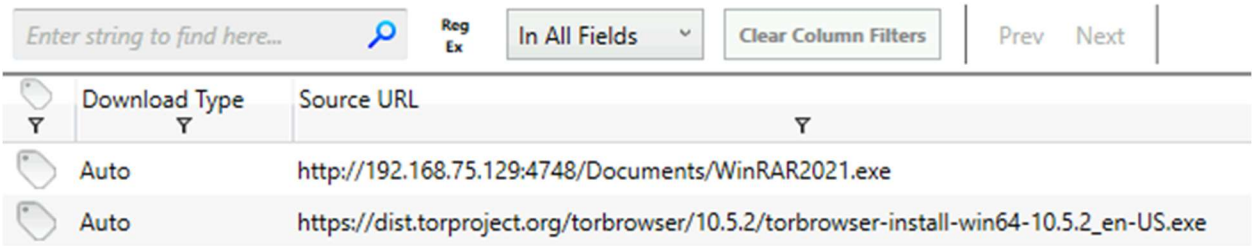
1st & 2nd Flag

Go to system Information tab and check there



3rd and 4th Flag

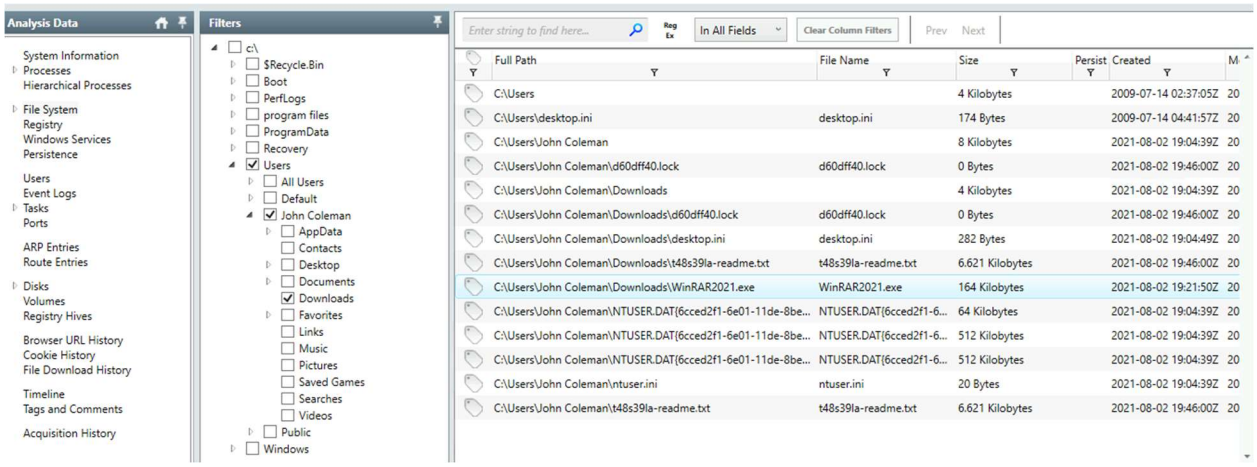
By going to file download history as mentioned in hints we can see WINRARsomething.exe and its URL.



5th and 6th Flag

Going on File system ➔Users ➔ John Coleman ➔ Downloads ➔ WinRar2021.exe

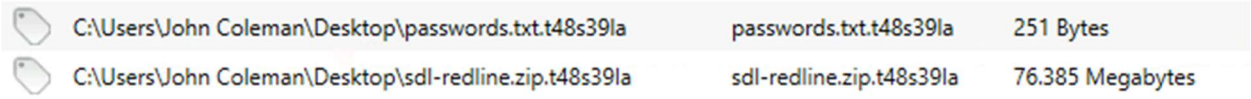
we can view the hash value and the size in kilobytes.



7th Flag

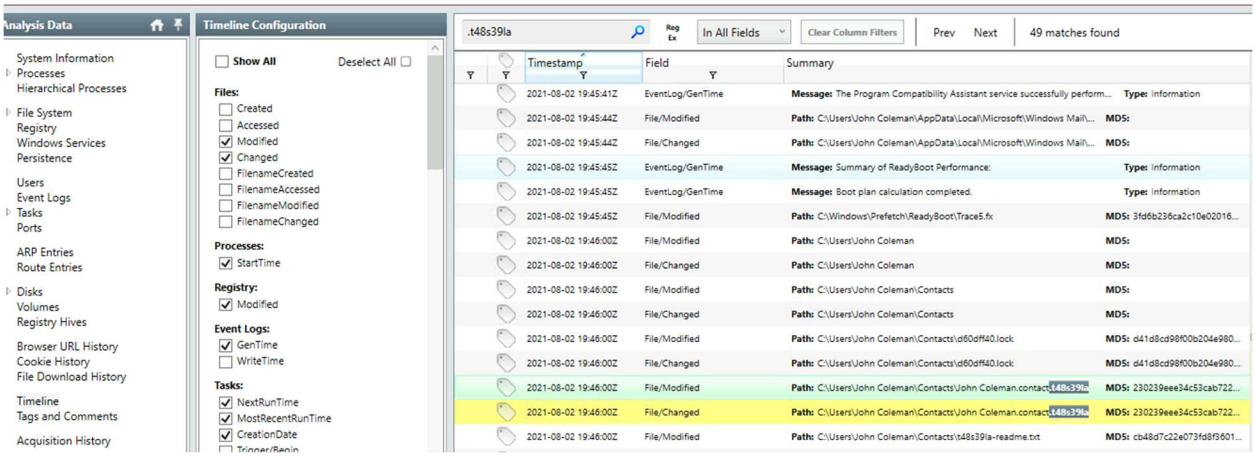
Go to File system ➔Users ➔ John Coleman ➔ Desktop.

We can see two files with .zip.something .txt.something file and as per the hint our flag is the .something extension shown below.



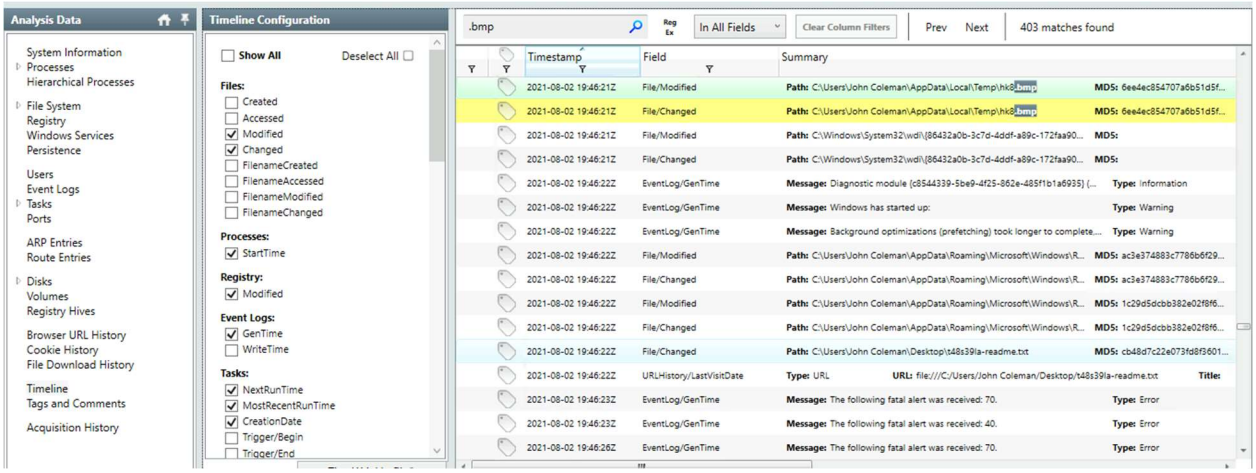
8th Flag

Go to Timeline and under Files select Modified and changed only and in search bar type the extension from our previous answer and the answer is (matches found – 1).



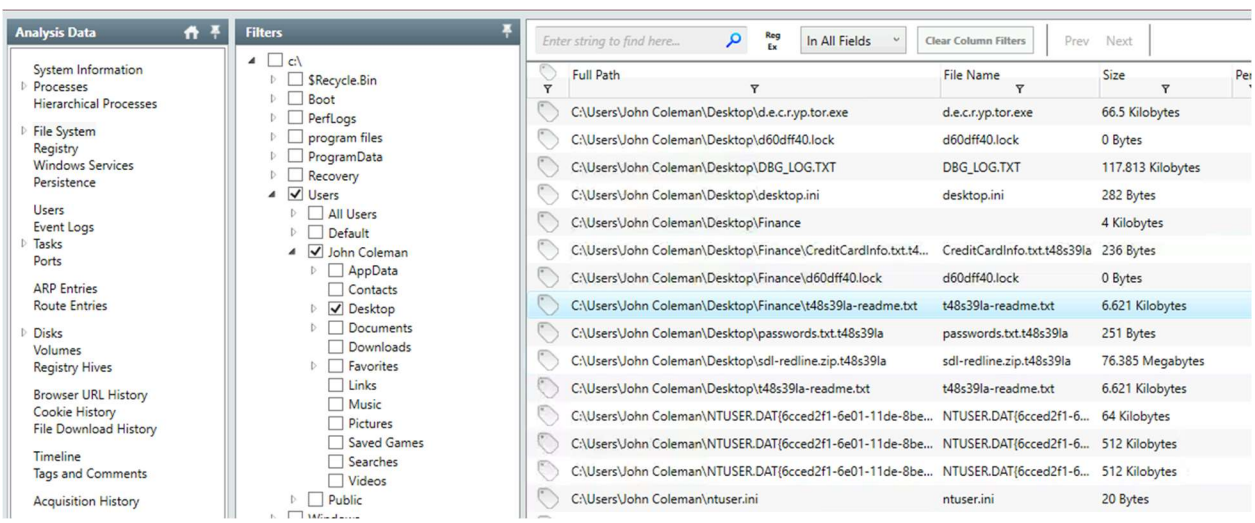
9th Flag

Same as above. Except search for .bmp extension and u will get the flag.



10th Flag

Go to File system ➔Users ➔ John Coleman and click on Desktop. Then u will see an readme file and that Is the answer for the question.



11th Flag

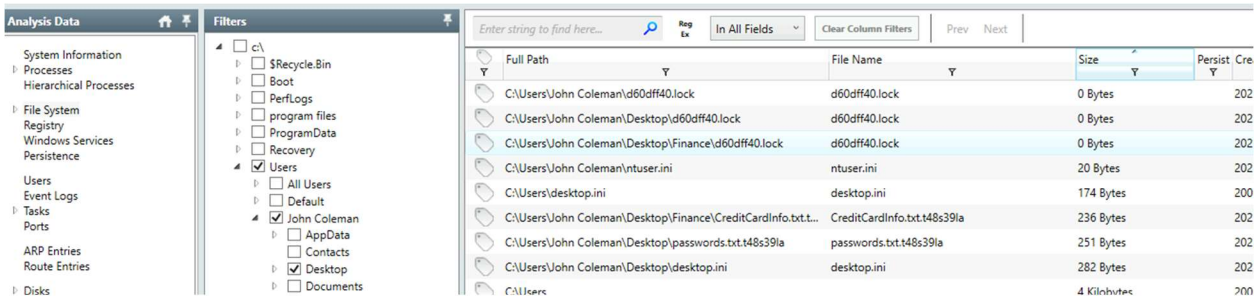
By going to path mention in the question we can easily see the name of file

C:\Users\John Coleman\Favorites\Links for United States\GobiernoUSA.gov.url.t48s39la	GobiernoUSA.gov.url.t48s39la

12th Flag:

File system ➔Users ➔ John Coleman ➔ Desktop

Check at size row.



13th Flag

By following the hint, we can easily retrieve the answer.

C:\Users\John Coleman\Desktop\d.e.c.r.yp.tor.exe	d.e.c.r.yp.tor.exe	66.5 Kilobytes

14th Flag

Going to Browser URL history we can see some (file://URL). That is done when uploading file from the PC and above it we can see the website URL. By checking above we can get the full URL required by our question.

URL	http://decryptor.top/favicon.ico
URL	file:///C:/Users/John Coleman/Documents/tesd/Sessi...
URL	file:///C:/Users/John Coleman/Desktop/t48s39la-read...
URL	file:///C:/Users/John Coleman/Desktop/passwords.txt
URL	file:///C:/Users/John Coleman/Desktop/sdl-redline.zip
URL	file:///C:/Users/John Coleman/Desktop/Finance/Credi...

http://decryptor.top/644E7C8EFA02FBB7

15th Flag

By doing some google search we can get the answer. One can check at virustotal, alienvault, mitre etc.