

1st & 2nd Flag

Go to system Information tab and check there

The screenshot shows the 'System Information' tab in a security tool. The left sidebar lists various system components like Processes, File System, Registry, Users, and more. The main content area is divided into several sections: Containment State, BIOS Information, Operating System Information, and User Information.

Containment State	
Containment State:	normal
Clock Skew:	00:00:00
State Agent Status:	monitoring_disabled

BIOS Information	
BIOS Date String:	07/22/20
BIOS Version:	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
BIOS Type:	BIOS

Operating System Information	
Operating System:	Windows 7 Home Premium 7601 Service Pack 1
Product Name:	Windows 7 Home Premium
Patch Level:	Service Pack 1
OS Build:	7601
Product ID:	00359-112-0000007-85772
System directory:	C:\Windows\system32
Install Date:	2021-08-02 19:04:38Z
Operating System Bitness:	32-bit

User Information	
Registered Owner:	Windows User
Registered Organization:	Not Available
Domain:	WORKGROUP
Logged in User:	John Coleman
Logged on User:	WIN-HKKQB6M7FTQ\John Coleman,WORKGROUP\WIN-HKKQB6M7FTQ\$

3rd and 4th Flag

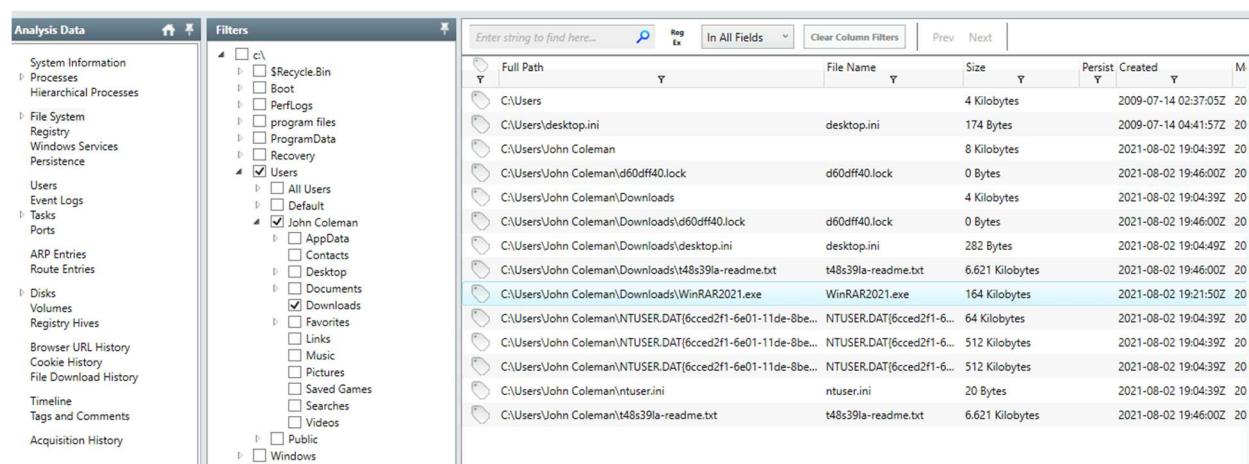
By going to file download history as mentioned in hints we can see WINRARsomething.exe and its URL.

Enter string to find here...		Reg Ex	In All Fields	Clear Column Filters	Prev	Next
Download Type	Source URL					
Auto	http://192.168.75.129:4748/Documents/WinRAR2021.exe					
Auto	https://dist.torproject.org/torbrowser/10.5.2/torbrowser-install-win64-10.5.2_en-US.exe					

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.



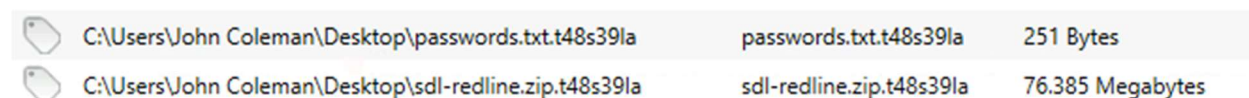
The screenshot shows a file system analysis tool with a left sidebar for navigation and a main table of files. The sidebar is expanded to 'Users' and then 'John Coleman', with 'Downloads' selected. The main table lists files with columns for Full Path, File Name, Size, Persist, Created, and M. The file 'WinRAR2021.exe' is highlighted in blue.

Full Path	File Name	Size	Persist	Created	M
C:\Users		4 Kilobytes		2009-07-14 02:37:05Z	20
C:\Users\desktop.ini	desktop.ini	174 Bytes		2009-07-14 04:41:57Z	20
C:\Users\John Coleman		8 Kilobytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\d60dff40.lock	d60dff40.lock	0 Bytes		2021-08-02 19:46:00Z	20
C:\Users\John Coleman\Downloads		4 Kilobytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes		2021-08-02 19:46:00Z	20
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes		2021-08-02 19:04:49Z	20
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-02 19:46:00Z	20
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	164 Kilobytes		2021-08-02 19:21:50Z	20
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	64 Kilobytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes		2021-08-02 19:04:39Z	20
C:\Users\John Coleman\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-02 19:46:00Z	20

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.



The screenshot shows a file system analysis tool with a left sidebar for navigation and a main table of files. The sidebar is expanded to 'Users' and then 'John Coleman', with 'Desktop' selected. The main table lists files with columns for Full Path, File Name, and Size. Two files are highlighted in blue.

Full Path	File Name	Size
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la	sdl-redline.zip.t48s39la	76.385 Megabytes

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).

Timestamp	Field	Summary
2021-08-02 19:45:41Z	EventLog/GenTime	Message: The Program Compatibility Assistant service successfully perform... Type: Information
2021-08-02 19:45:44Z	File/Modified	Path: C:\Users\John Coleman\AppData\Local\Microsoft\Windows Mail... MDS: 3f05b236ca2c10e02016...
2021-08-02 19:45:44Z	File/Changed	Path: C:\Users\John Coleman\AppData\Local\Microsoft\Windows Mail... MDS: 3f05b236ca2c10e02016...
2021-08-02 19:45:45Z	EventLog/GenTime	Message: Summary of ReadyBoot Performance: Type: Information
2021-08-02 19:45:45Z	EventLog/GenTime	Message: Boot plan calculation completed. Type: Information
2021-08-02 19:45:45Z	File/Modified	Path: C:\Windows\Prefetch\ReadyBoot\Trace5.fx MDS: 3f05b236ca2c10e02016...
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman MDS: 3f05b236ca2c10e02016...
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman MDS: 3f05b236ca2c10e02016...
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts MDS: 3f05b236ca2c10e02016...
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman\Contacts MDS: 3f05b236ca2c10e02016...
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts\id60d940.lock MDS: d41d8cd98f00b204e980...
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman\Contacts\id60d940.lock MDS: d41d8cd98f00b204e980...
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts\John Coleman.contact.t48s39la MDS: 230239eee34c53cab722...
2021-08-02 19:46:00Z	File/Changed	Path: C:\Users\John Coleman\Contacts\John Coleman.contact.t48s39la MDS: 230239eee34c53cab722...
2021-08-02 19:46:00Z	File/Modified	Path: C:\Users\John Coleman\Contacts\id68s39la-readme.txt MDS: cb48d7c22e073f8f9601...

9th Flag

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

11th Flag

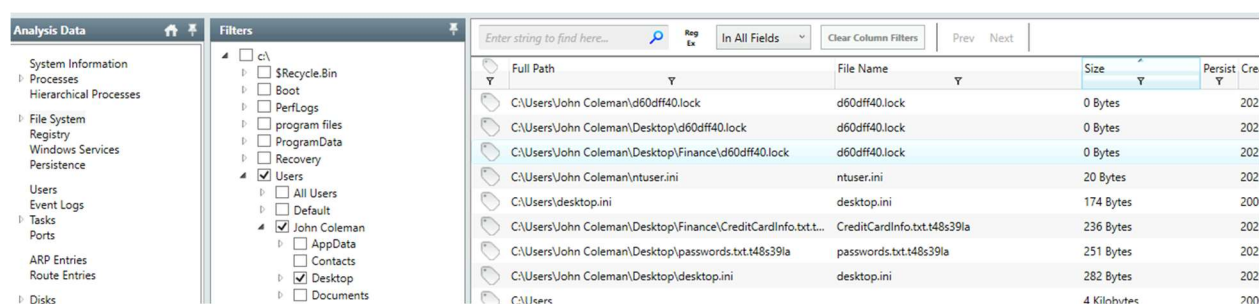
By going to path mention in the question we can easily see the name of file

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.



Full Path	File Name	Size	Persist	Cre
C:\Users\John Coleman\d60dff40.lock	d60dff40.lock	0 Bytes		202
C:\Users\John Coleman\Desktop\d60dff40.lock	d60dff40.lock	0 Bytes		202
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock	d60dff40.lock	0 Bytes		202
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes		202
C:\Users\John Coleman\Desktop\ini	desktop.ini	174 Bytes		200
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t...	CreditCardInfo.txt.t48s39la	236 Bytes		202
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes		202
C:\Users\John Coleman\Desktop\desktop.ini	desktop.ini	282 Bytes		202
C:\Users\John Coleman\Desktop\...	...	4 Kilobytes		200







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.