DIGITAL FORENSICS LAB

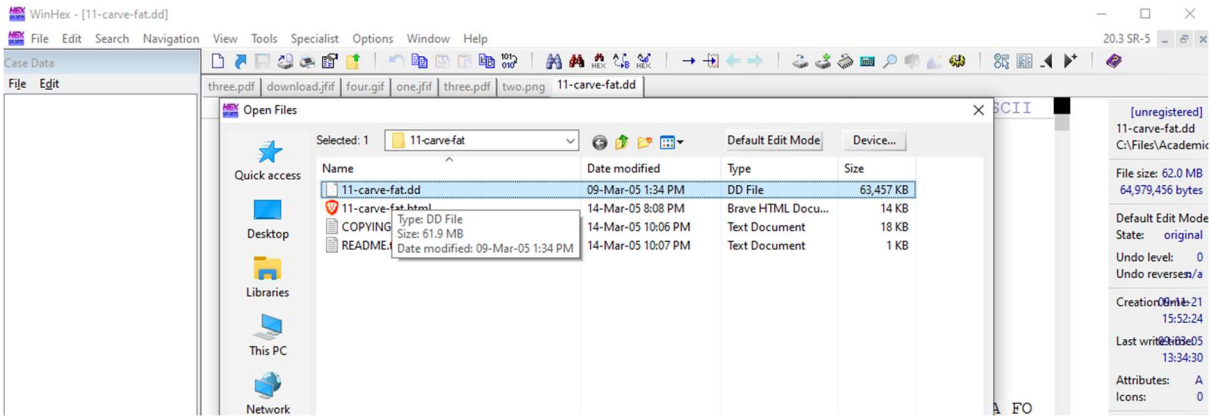
Exercise 11	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	9th November, 2021

AIM

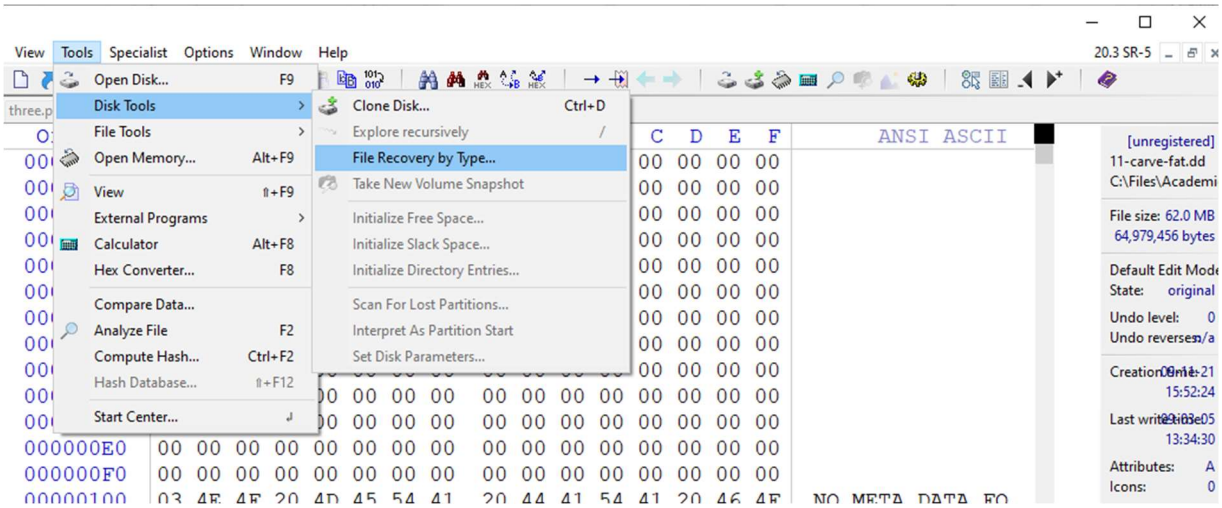
Performing Data/File carving on a couple disk images

PROCESS

1. Open the image (the DD file) using WinHex.

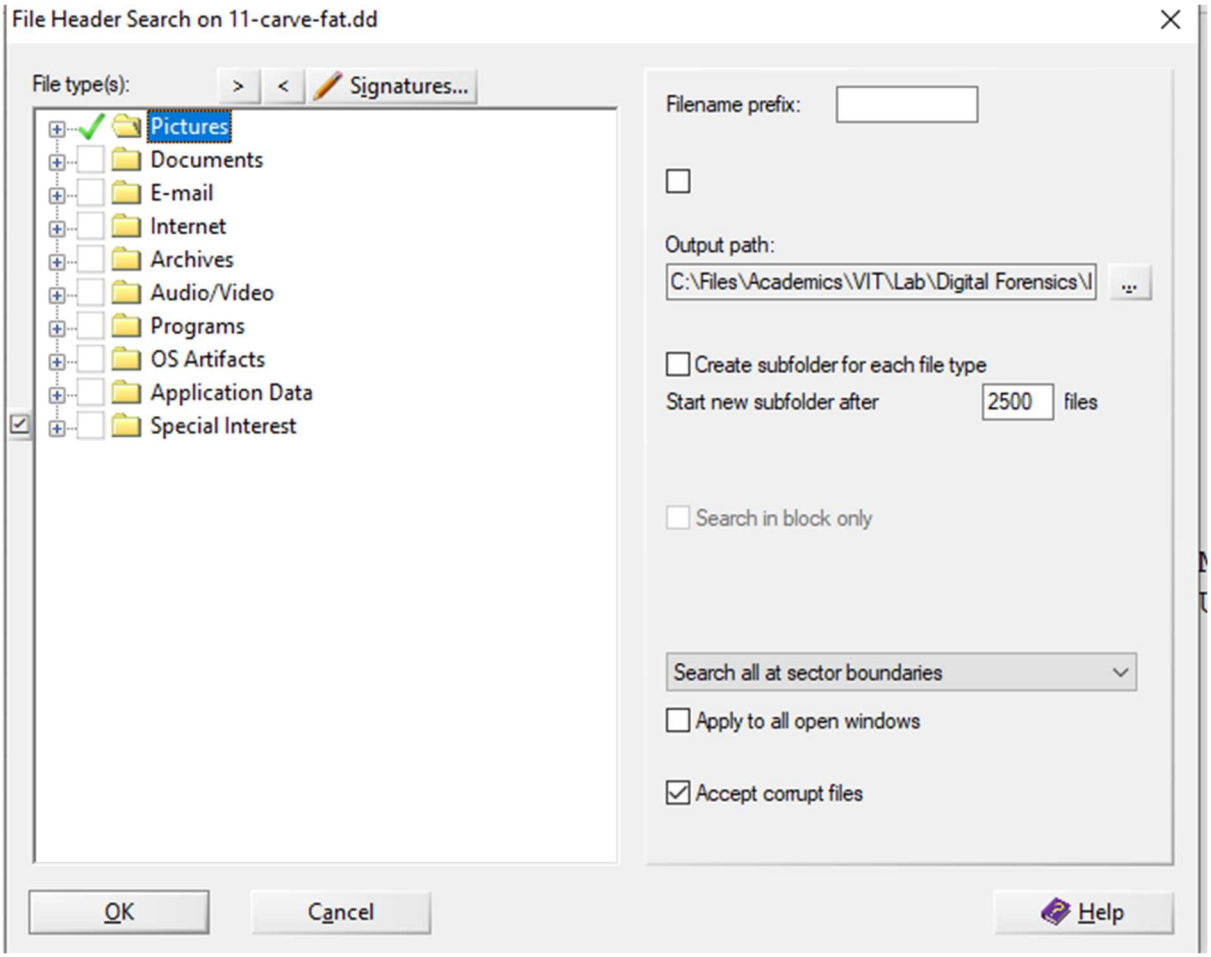


2. Next go to Tools>Disk Tools>File Recovery by Type…

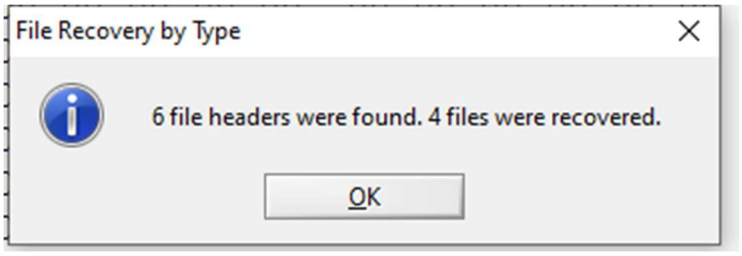


3. Select the type of files you would like to recover (like Pictures, Audio etc). We can also specify what kinds of extensions to recover by

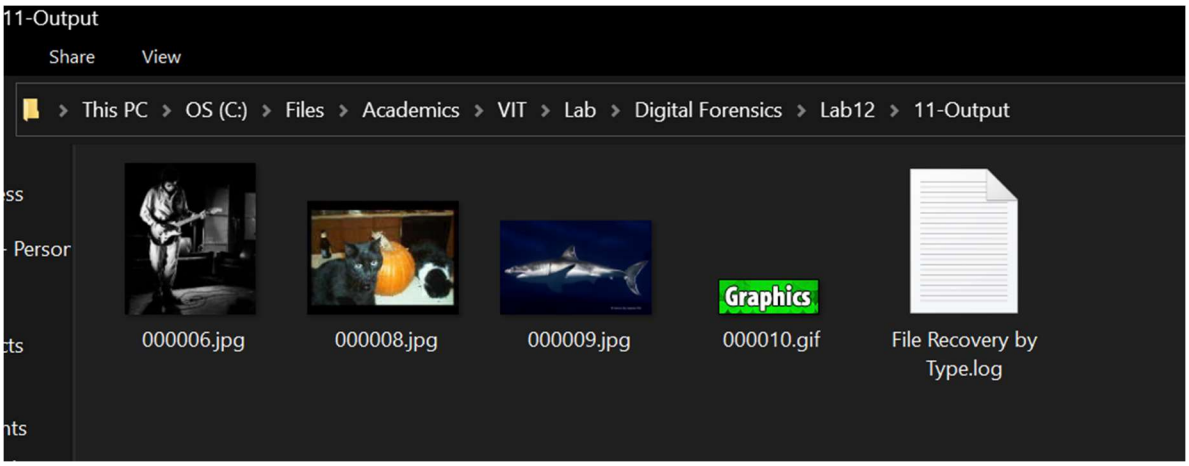
expanding each file type. Also select the Output path where the recovered files are supposed to be saved. Then click ‘OK’.



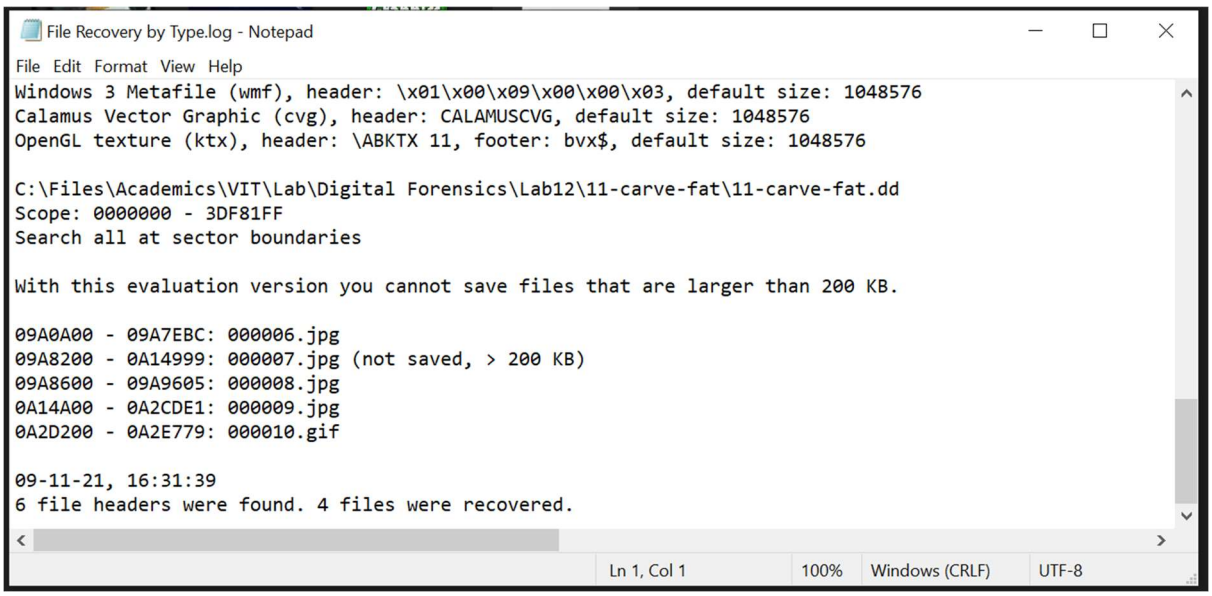
4. Upon completion, the program will display a pop-up as follows. In case of this image file, we find 6 headers out of which WinHex was able to recover 4 image files.



5. Go to the output folder and check the recovered files.



6. We can open the log file to see which files were not recovered. The current evaluation of WinHex used (trial version) does not save files bigger than 200 KB. So, one of the files could not be recovered due to licensing restriction. The log is as shown below.



OBSERVATIONS

Image 1 – Image of a FAT disk

The image used here is that of a FAT disk. It had the following list of files which were then deleted:

Num	Name	MD5	Size	Note	Sectors
1	2003_document.doc	e72f388b36f9370f19696b164c308482	19968	A Valid DOC file	(0-38) 281 -320
2	enterprise.wav	7629b89adade055f6783dc1773274215	318895	A valid WAV file	(0-622) 16021 -16644
3	haxor2.jpg	84e1dceac2eb127fef5bfdcb0eae324b	24367	An invalid JPEG with only 1 header byte corrupted. This byte is located at offset 19 within the file.	(0-47)16645 -16692
4	holly.xls	7917baf0219645afef8b381570c41211	23040	A valid XLS file	(0-44) 16693-16738
5	lin_1.2.pdf	e026ec863410725ba1f5765a1874800d	1399508	A linearized PDF	(0-2733) 16741 -19475
6	nlin_14.pdf	5b3e806e8c9c06a475cd45bf821af709	122434	A non-linearized PDF	(0-239) 19477 -19716
7	paul.jpg	37a49f97ed279832cd4f7bd002c826a2	29885	A valid jpeg	(0-58) 19717 -19776
8	pumpkin.jpg	6c9859e5121ff54d5d6298f65f0bf3b3	444314	A valid EXIF jpeg	(0-867) 19777-20644
9	shark.jpg	d83428b8742a075b57b0dc424cd297c4	99298	A valid JPEG	(0-193) 20645-20839
10	sml.gif	d25fb845e6a41395adaed8bd14db7bf2	5498	A valid GIF	(0-10) 20841-20852
11	surf.mov	5328d2b066f428ea95b2793849ab97fa	550653	A valid MOV	(0-1075) 20853-21928
12	surf.wmv	ff085d0c4d0e0fdc8f3427db68e26266	1036994	A valid WMV	(0-2025) 21929-23955
13	test.ppt	7b74c2c608d92f4bb76c1d3b6bd1decc	11264	A deleted PPT	(0-21) 23957 -23978
14	wword60t.zip	c0be59d49b7ee0fdc492d2df32f2c6c6	78899	A valid ZIP	(0-154) 23981 -24135
15	domopers.wmv	63c0c6986cf0a446cb54b0ac65a921a5	8037267	A deleted wmv	(0-15697) 321-16018

Using WinHex, we try and recover the deleted files by following the process above.

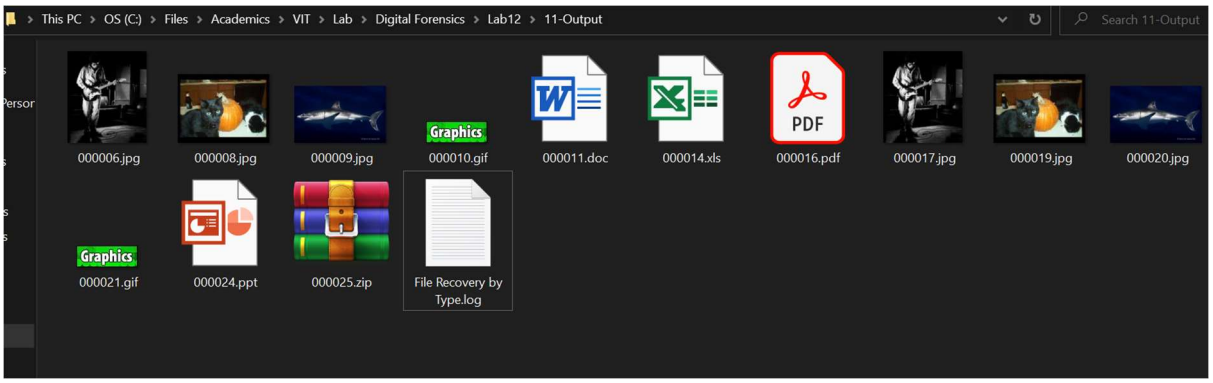


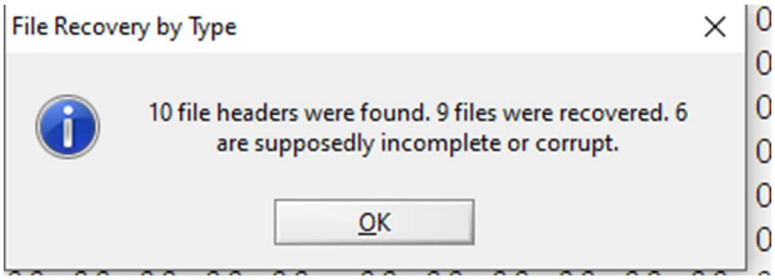
Image 2 – Image of a EXT2 disk

The image used here is that of a EXT2 disk. It had the following list of files which were then deleted:

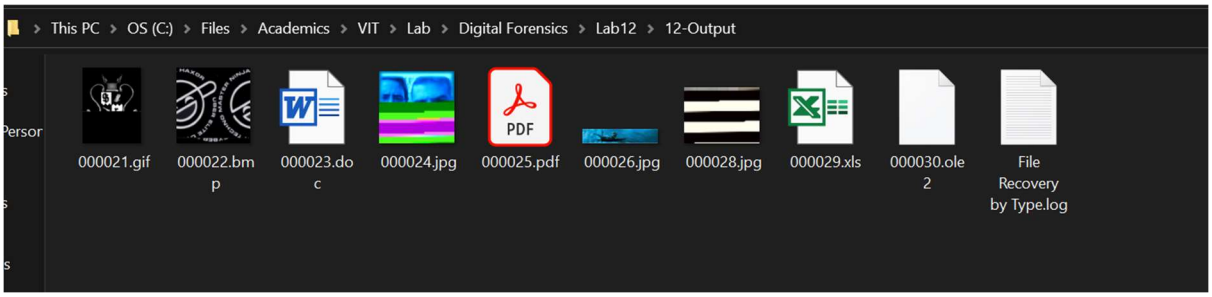
Num	Name	MD5	Size	Note	Sectors
1	haxor2.bmp	f9633fe6b9ef2a0a5edd6de70d22c0f5	163878	A deleted BMP	(0-22):5162-5184, (IND):5186, (24-320):518
2	jimmy.doc	2f3f914dd74819df42d1d941c7275c16	12800	A deleted DOC	(0-22):5486-5508, (IND):5510, (24):551
3	jn.jpg	270a0a913fa9603db8121fdf78d63aca	28949	A valid JPG	(0-22):5514-5536, (IND):5538, (24-56):5540
4	lin_test.pdf	1c64456776075d1f0a662e1f6c09e340	26618	A valid PDF	(0-22):5574-5596, (IND):5598, (24-50):5600
5	main_dive.jpg	937846adb96773ee25fcb34821230976	8463	A valid jpeg	(0-16):5628-5644
6	n_lin_ss.pdf	97be95ed3e710b63bc75e5c0775062d9	734652	A valid pdf	(0-22):5646-5668, (IND):5670, (24-534):5672-6182, (DIND):6184, (IN (IND):6700, (1048-1434)6702-7088
7	blogo.gif	5e10b2176016885a85bffc074a142524	18663	A valid gif	(0-22):5122-5144, (IND):5146, (24-36):5148
8	sherry.jpg	3834e72d2ee266ccfb9733d716b89f2b	133249	A valid JPEG	(0-22):7090-7112, (IND):7114, (24-260):711
9	stats.xls	6351df9c1543c41c3df8eea63e06a219	15360	A valid XLS	(0-22):7354-7376, (IND):7378, (24-28):7380
10	test.ppt	99941c129cc8cfbadc15c55086982efc	17408	A valid PPT	(0-22):7386-7408, (IND):7410, (24-32):7412

Using WinHex, we try and recover the deleted files by following the process above.

Deleted files which were supported by WinHex could be recovered. However, due to the limits the lack of licensing poses, we extract only files that are smaller than 200 KB. Out of the 10 files detected, 9 were recovered. 6 of them appear to be incomplete or corrupt according to WinHex.



All files recovered from the second image are the following:



CONCLUSION

The deleted files were recovered using file/data carving with the aid of WinHex.

DIGITAL FORENSICS LAB

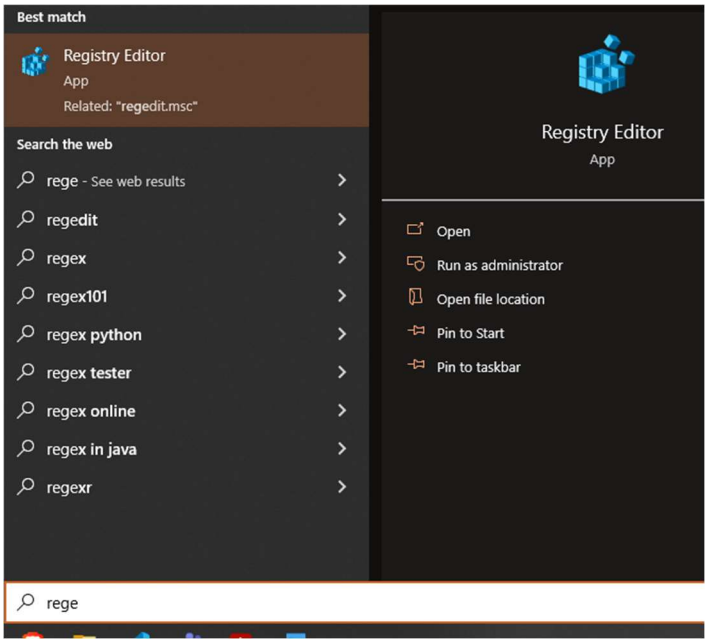
Exercise 12	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	23rd November, 2021

AIM

Exploring the windows registry keys and values.

PROCESS

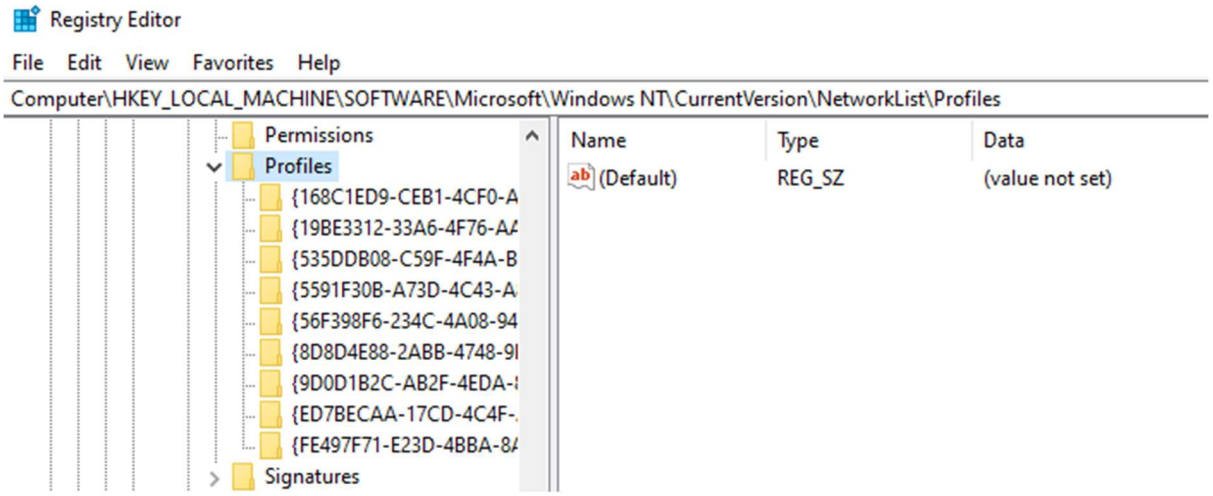
1. Open up 'Run' or press the windows key.
2. Search for Regedit.
3. Open the 'Registry Editor'.

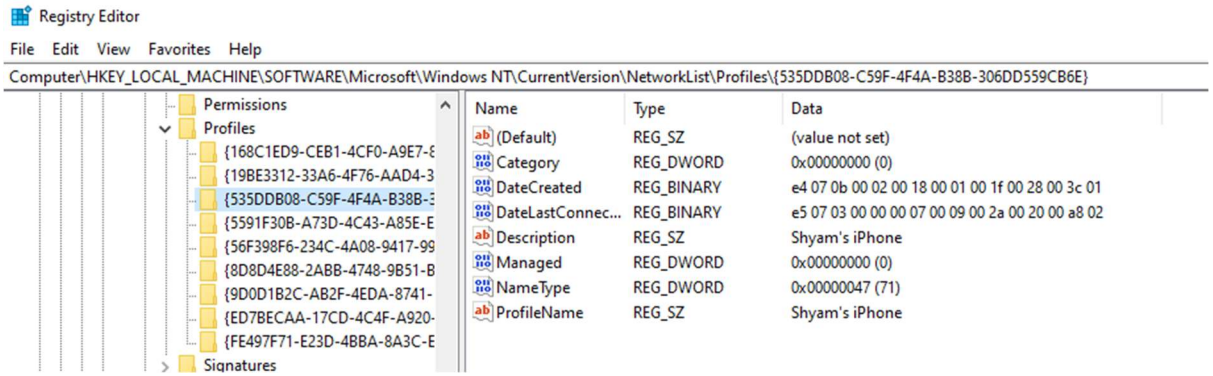


OBSERVATIONS

List of GUIDs of Wireless access points connected

Path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\



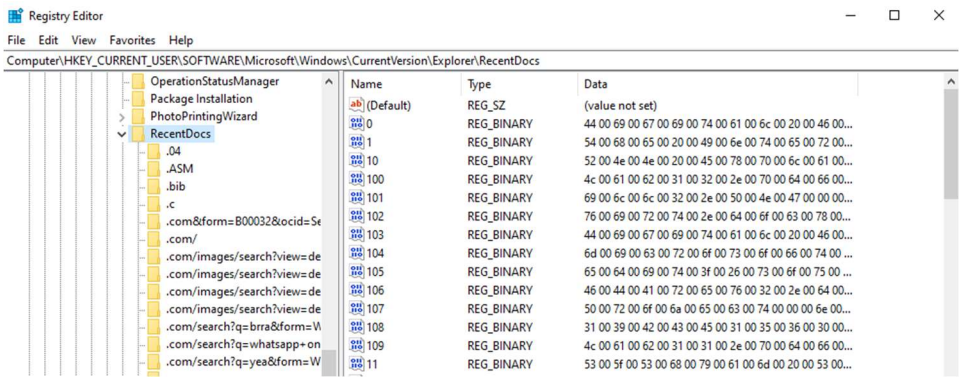


It shows the list of networks connected to in the past in folders. In the screenshot we see that one of the networks was an iPhone's hotspot.

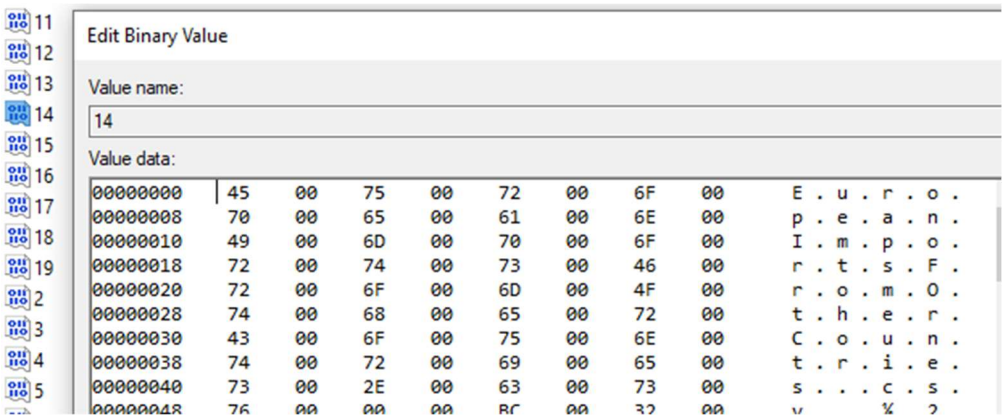
Recent Documents

Path:

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



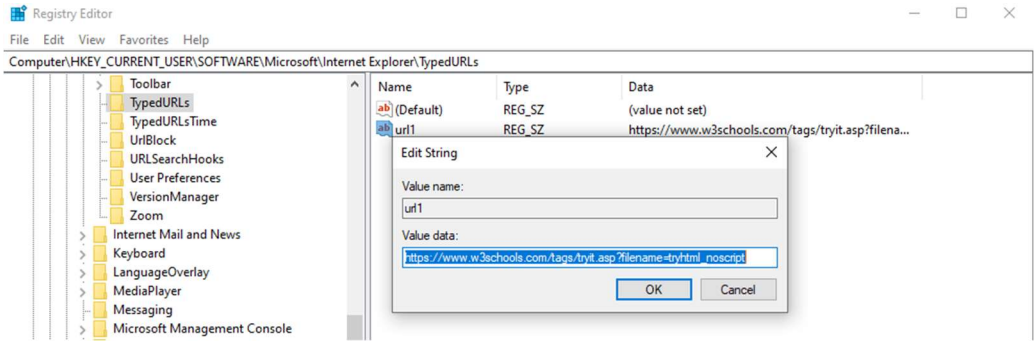
We can see a list of file types, each containing details of files accessed. We can also see the names. For example, below is an entry with the name of the CSV file accessed in the rightmost column.



It reads ‘EuropeanImportsFromOtherCountries’. This is a CSV file used for FDA lab.

URLS typed in internet explorer

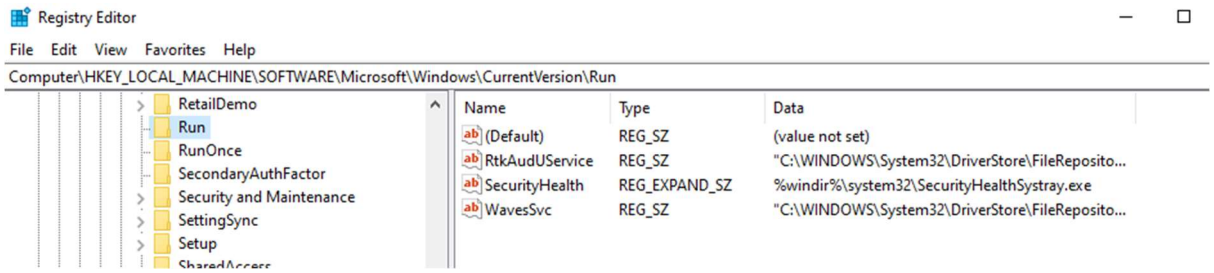
Path: Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs



Applications Run when system starts

Path:

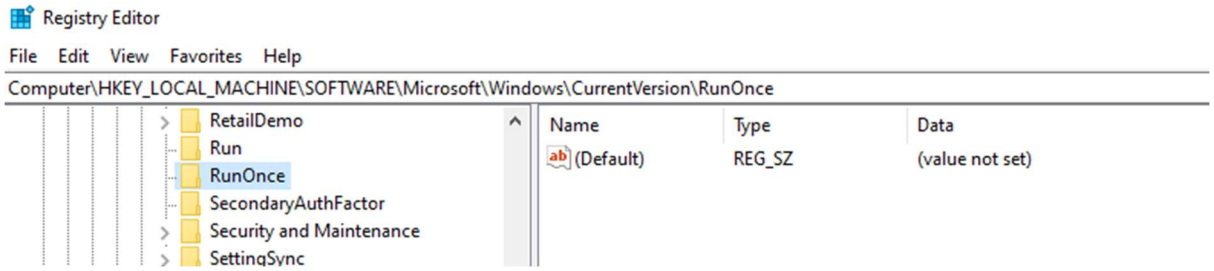
Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



Applications Run Once

Path:

Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

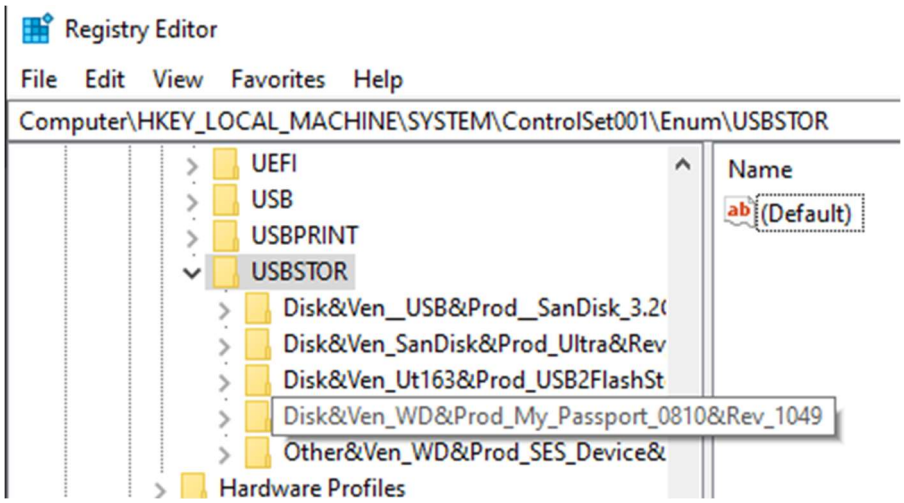


There are no such applications.

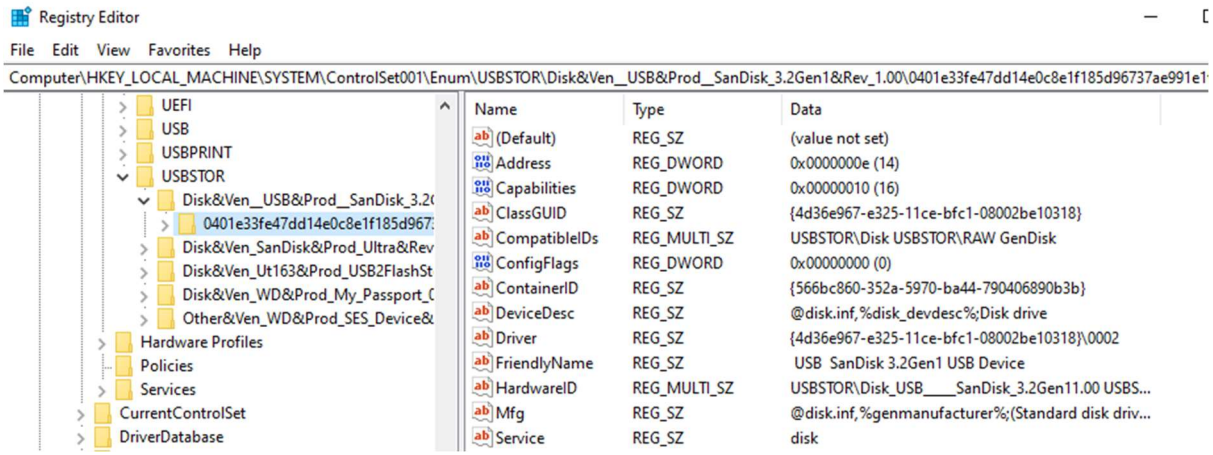
Check if USB was inserted

Path:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

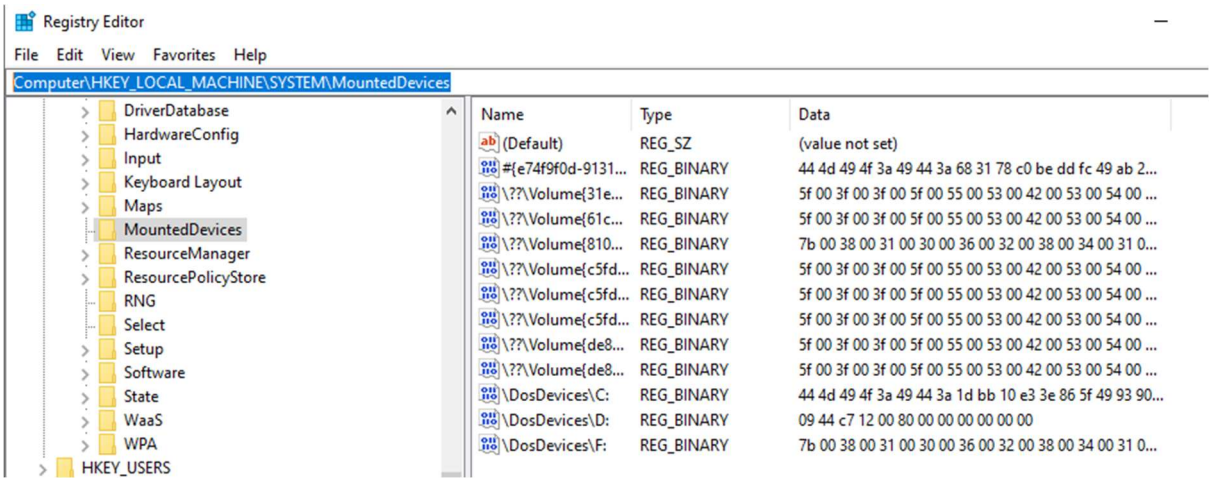


Each device inserted has its own sub-folder. The contents of one of them are shown below:



Check for devices that were mounted

Path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices



CONCLUSION

Thus, we have seen a handful of samples regarding the kinds of information that can be extracted about a device from its registry.