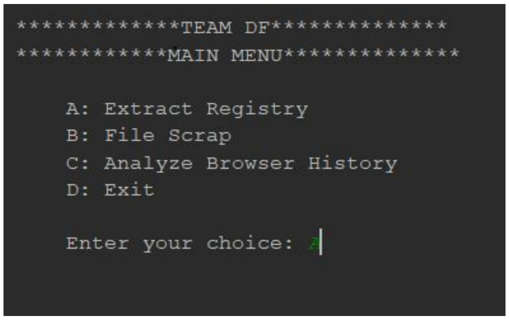
User Manual

Function A: Registry Extraction

Running the program

Step 1: Enter ‘A’ when the below options are shown

*Main Menu input is not case sensitive

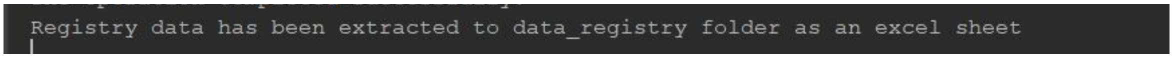


```
*************TEAM DF**************
************MAIN MENU**************


    A: Extract Registry
    B: File Scrap
    C: Analyze Browser History
    D: Exit

    Enter your choice: A
```

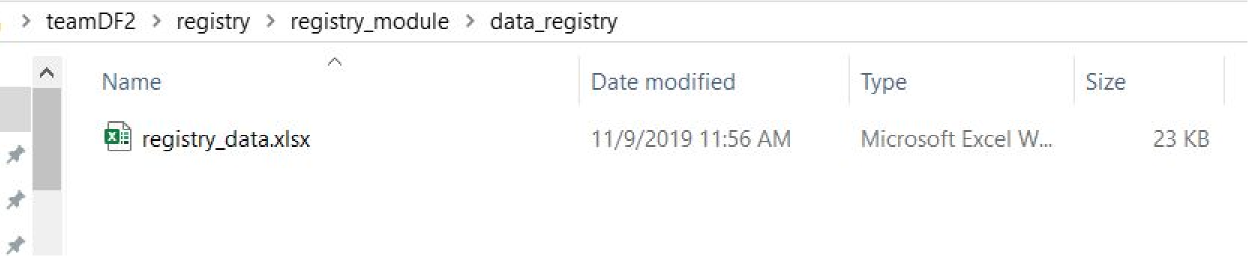
Step 2: Once user has entered his choice, the following output will be shown:



```
  Registry data has been extracted to data_registry folder as an excel sheet
```

Step 3: User will have to access the data_registry folder at the file path that he has set in the config.json file for the data_file_path variable.

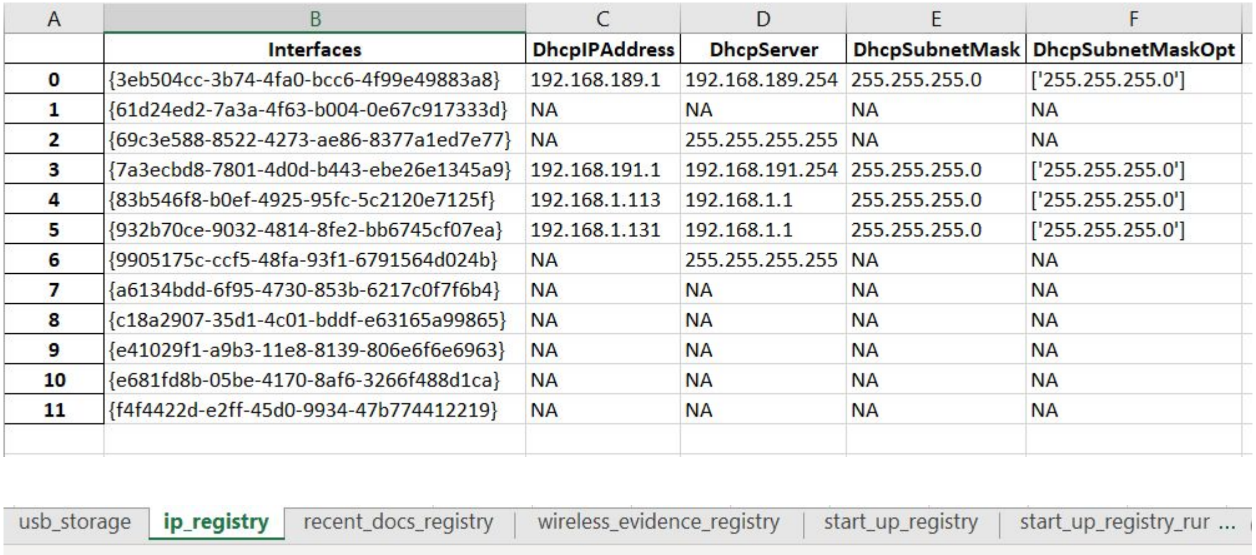
User needs to go into the registry folder → registry_module folder → data_registry folder. When user have reached the folder, if registry data has been successfully extracted, it will output to an excel file, ‘registry_data.xslx’ as can be seen below:



> teamDF2 > registry > registry_module > data_registry

Name	Date modified	Type	Size
registry_data.xlsx	11/9/2019 11:56 AM	Microsoft Excel W...	23 KB

Step 4: Once User opens the registry_data.xlsx, the layout should look something similar to this because different people have different information on their registry. There should be a total of 6 different sheets in the excel page. The sheets are “usb_storage, ip_registry, recent_docs_registry, wireless_evidence_registry, start_up_registry, start_up_registry_run_once, startup_particular_user”.



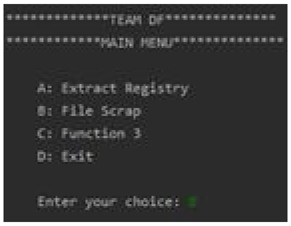
	Interfaces	DhcpIPAddress	DhcpServer	DhcpSubnetMask	DhcpSubnetMaskOpt
0	{3eb504cc-3b74-4fa0-bcc6-4f99e49883a8}	192.168.189.1	192.168.189.254	255.255.255.0	['255.255.255.0']
1	{61d24ed2-7a3a-4f63-b004-0e67c917333d}	NA	NA	NA	NA
2	{69c3e588-8522-4273-ae86-8377a1ed7e77}	NA	255.255.255.255	NA	NA
3	{7a3ecbd8-7801-4d0d-b443-ebe26e1345a9}	192.168.191.1	192.168.191.254	255.255.255.0	['255.255.255.0']
4	{83b546f8-b0ef-4925-95fc-5c2120e7125f}	192.168.1.113	192.168.1.1	255.255.255.0	['255.255.255.0']
5	{932b70ce-9032-4814-8fe2-bb6745cf07ea}	192.168.1.131	192.168.1.1	255.255.255.0	['255.255.255.0']
6	{9905175c-ccf5-48fa-93f1-6791564d024b}	NA	255.255.255.255	NA	NA
7	{a6134bdd-6f95-4730-853b-6217c0f7f6b4}	NA	NA	NA	NA
8	{c18a2907-35d1-4c01-bddf-e63165a99865}	NA	NA	NA	NA
9	{e41029f1-a9b3-11e8-8139-806e6f6e6963}	NA	NA	NA	NA
10	{e681fd8b-05be-4170-8af6-3266f488d1ca}	NA	NA	NA	NA
11	{f4f4422d-e2ff-45d0-9934-47b774412219}	NA	NA	NA	NA

Function B : File Scrap

Running the program

Step 1: Enter ‘B’ when the below options are shown

*Main Menu input is not case sensitives



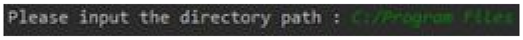
```
**************TEAM DF**************
************MAIN MENU**************

   A: Extract Registry
   B: File Scrap
   C: Function 3
   D: Exit

   Enter your choice: B
```

Step 2: Enter <yourTargetFileDirectorys> when system prompted as below:

*Input can be any valid path within the system

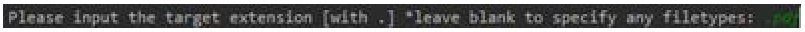


```
Please input the directory path : C:/Program Files
```

Step 3: Enter 1 <yourTargetFileExtension> when system prompted as below:

*list of available inputs and expected result

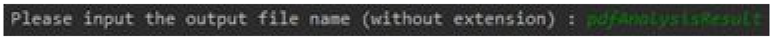
File Input	Result
Empty input (null)	output ALL files (with modified Date Time, categorization, File Path/Name) within the directory to CSV
.pdf	output ALL **pdf** files (with modified Date Time, categorization, File Path/Name) within the directory to CSV
.docx	output ALL **docx** files (with modified Date Time, categorization, File Path/Name) within the directory to CSV
.txt	output ALL **txt** files (with modified Date Time, categorization, File Path/Name) within the directory to CSV
.jpg	output ALL ***jpg*** files (with modified Date Time, File Path/Name, Metadata) within the directory to CSV
*valid Extension (E.g. .exe)	output ALL ***specificExt*** files (with modified Date Time, File Path/Name, Metadata) within the directory to CSV
*invalid Extension	output an empty CSV



```
Please input the target extension [with .] *leave blank to specify any filetypes: .pdf
```

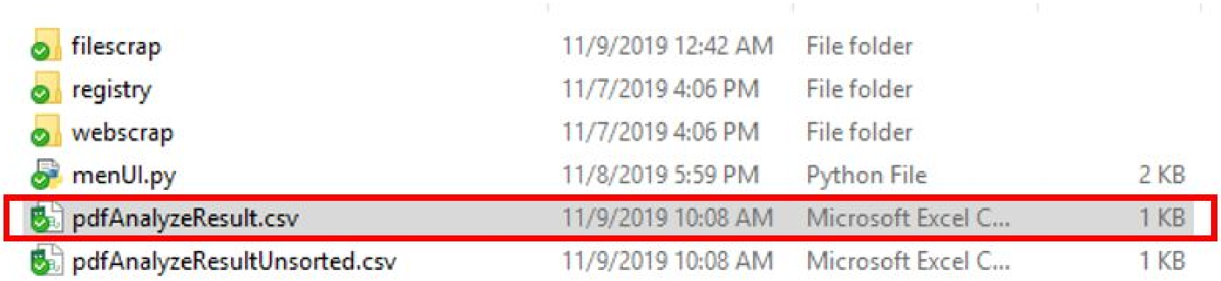
Step 4: Enter <yourOutputFileName> when system prompted as below:

*File name can be of user’s preferences



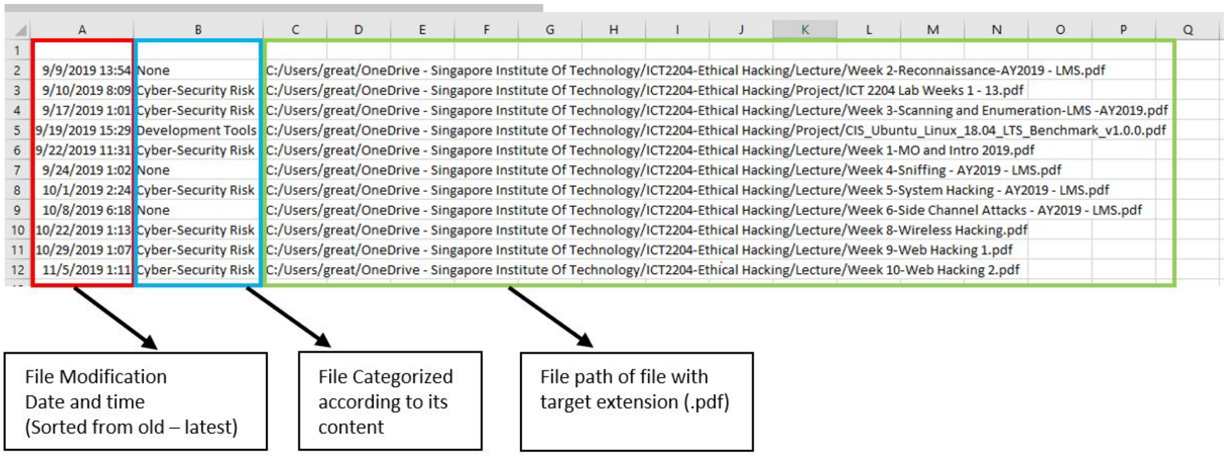
```
Please input the output file name (without extension) : pdfAnalysisResult
```

Step 5: Output file: <yourOutputFileName>.csv can be located in the same file directory and open with Microsoft Excel.



filescrap	11/9/2019 12:42 AM	File folder	
registry	11/7/2019 4:06 PM	File folder	
webscrap	11/7/2019 4:06 PM	File folder	
menUI.py	11/8/2019 5:59 PM	Python File	2 KB
pdfAnalyzeResult.csv	11/9/2019 10:08 AM	Microsoft Excel C...	1 KB
pdfAnalyzeResultUnsorted.csv	11/9/2019 10:08 AM	Microsoft Excel C...	1 KB

Step 6: Open the <yourOutputFileName>.csv



	A	B	C
1			
2	9/9/2019 13:54	None	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 2-Reconnaissance-AY2019 - LMS.pdf
3	9/10/2019 8:09	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Project/ICT 2204 Lab Weeks 1 - 13.pdf
4	9/17/2019 1:01	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 3-Scanning and Enumeration-LMS -AY2019.pdf
5	9/19/2019 15:29	Development Tools	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Project/CIS_Ubuntu_Linux_18.04_LTS_Benchmark_v1.0.0.pdf
6	9/22/2019 11:31	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 1-MO and Intro 2019.pdf
7	9/24/2019 1:02	None	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 4-Sniffing - AY2019 - LMS.pdf
8	10/1/2019 2:24	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 5-System Hacking - AY2019 - LMS.pdf
9	10/8/2019 6:18	None	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 6-Side Channel Attacks - AY2019 - LMS.pdf
10	10/22/2019 1:13	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 8-Wireless Hacking.pdf
11	10/29/2019 1:07	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 9-Web Hacking 1.pdf
12	11/5/2019 1:11	Cyber-Security Risk	C:/Users/great/OneDrive - Singapore Institute Of Technology/ICT2204-Ethical Hacking/Lecture/Week 10-Web Hacking 2.pdf

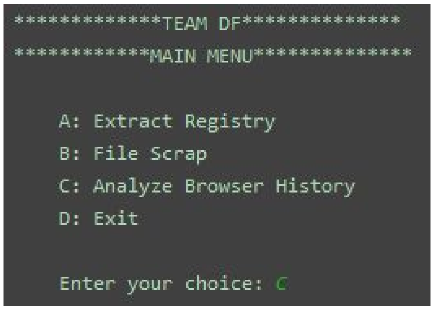
File Modification
Date and time
(Sorted from old – latest)

File Categorized
according to its
content

File path of file with
target extension (.pdf)

Function C: Analyze Browser History

Running Program

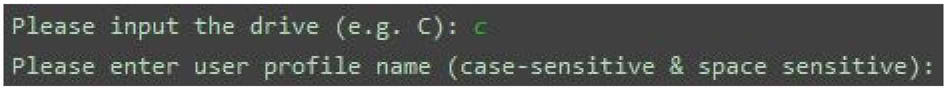


```
*************TEAM DF**************
************MAIN MENU*************

    A: Extract Registry
    B: File Scrap
    C: Analyze Browser History
    D: Exit

    Enter your choice: C
```

Input choice ‘C’ to run Analyze Browser History



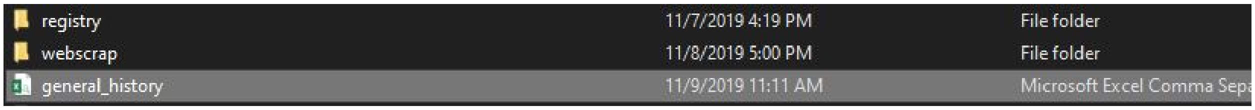
```
Please input the drive (e.g. C): c
Please enter user profile name (case-sensitive & space sensitive):
```

1) User have to specify the drive (e.g. C for C drive) where the internet browser (firefox,chrome) is located on

2) User also have to specify the name of the user for example in C drive (C:\Users\John)

3) User have to ensure browser is closed before the start of extraction of the browser history.

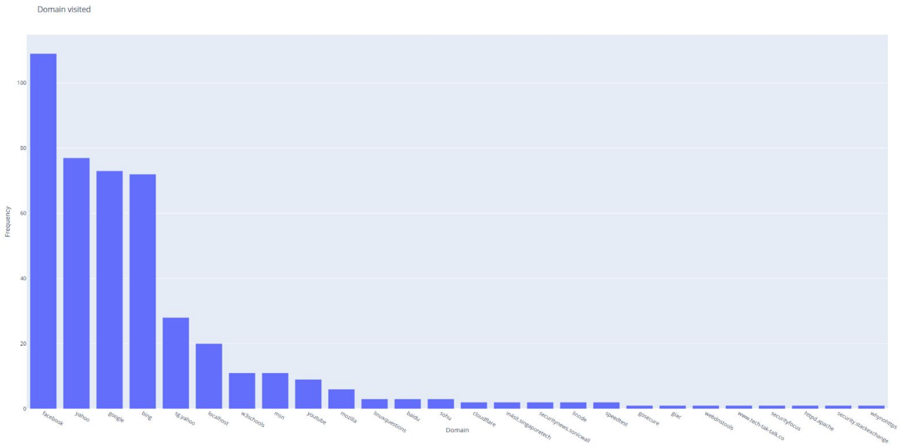
After the extraction of browser history, a CSV file called “general_history” will be saved to the directory



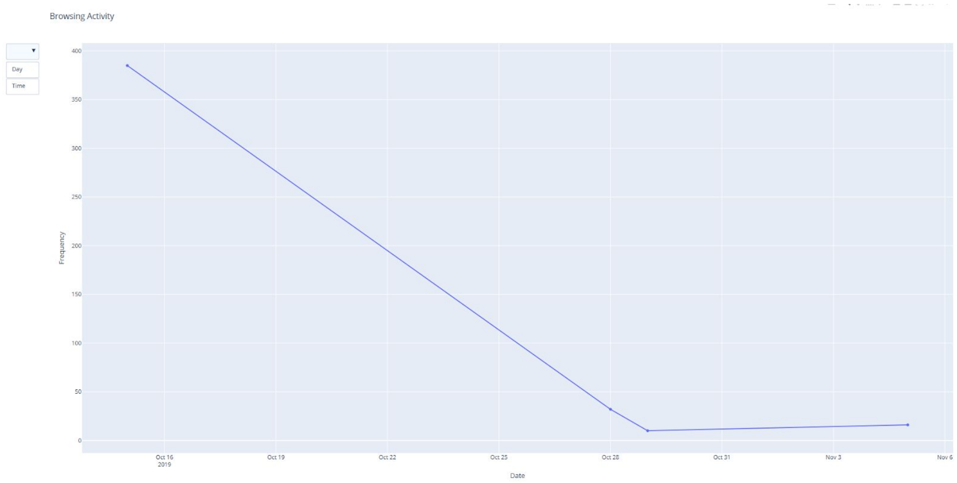
registry	11/7/2019 4:19 PM	File folder
webscrap	11/8/2019 5:00 PM	File folder
general_history	11/9/2019 11:11 AM	Microsoft Excel Comma Sepa

After CSV generated, the program will continue to execute to produce charts to visualize the data retrieved.

Two charts will be produced as follows:

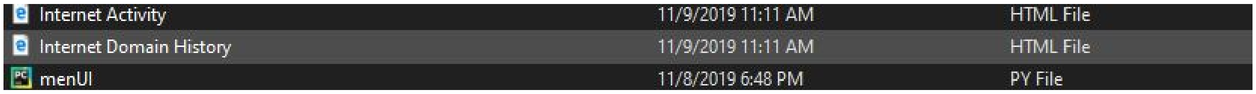


Domain visited



Internet Activity with the option to see timing or overall by date

The charts will be saved as html file called “Internet Activity” and “Internet Domain History” in the directory as well



Internet Activity	11/9/2019 11:11 AM	HTML File
Internet Domain History	11/9/2019 11:11 AM	HTML File
menUI	11/8/2019 6:48 PM	PY File