Malware Behavior Classification Using Deep Learning

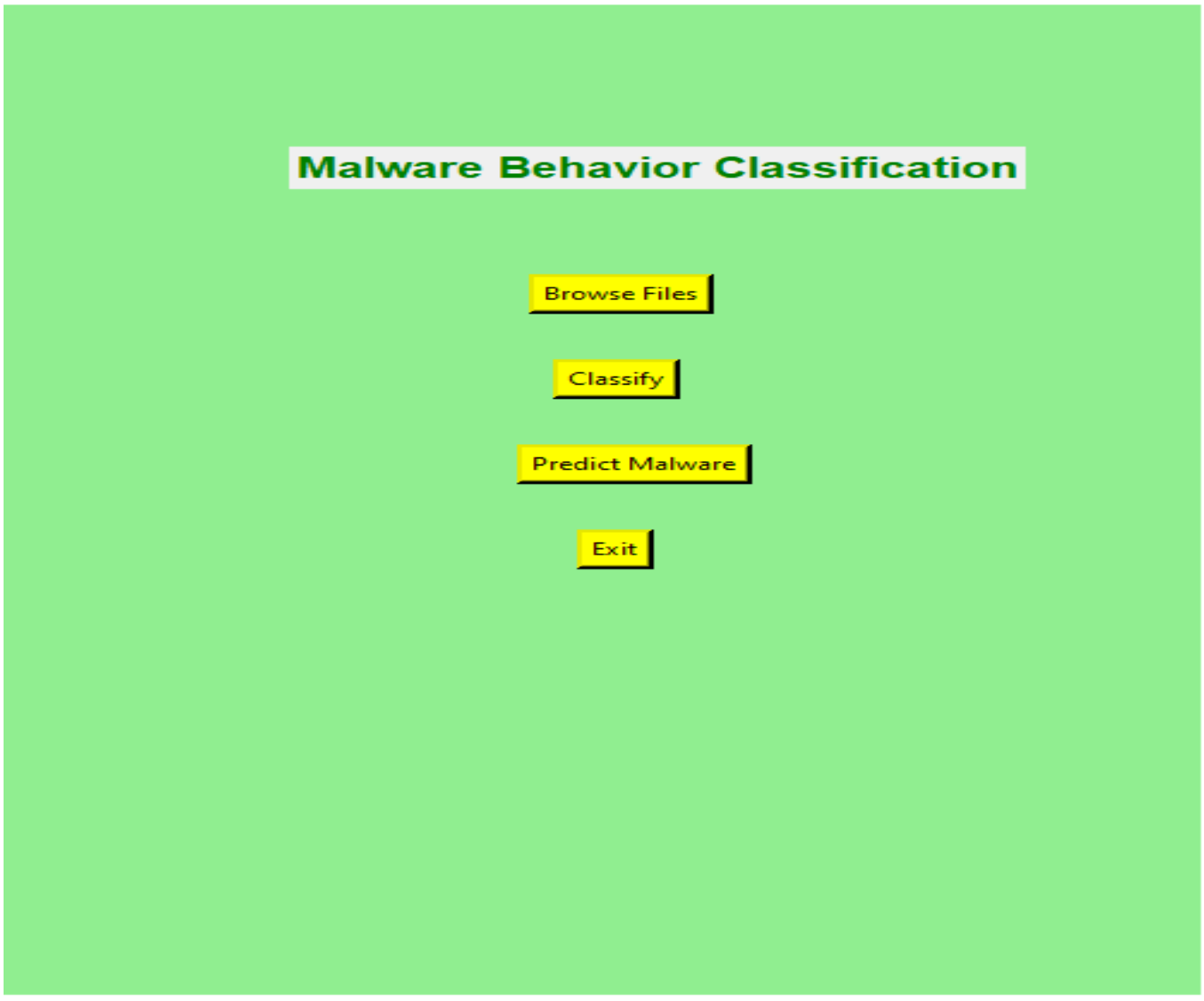
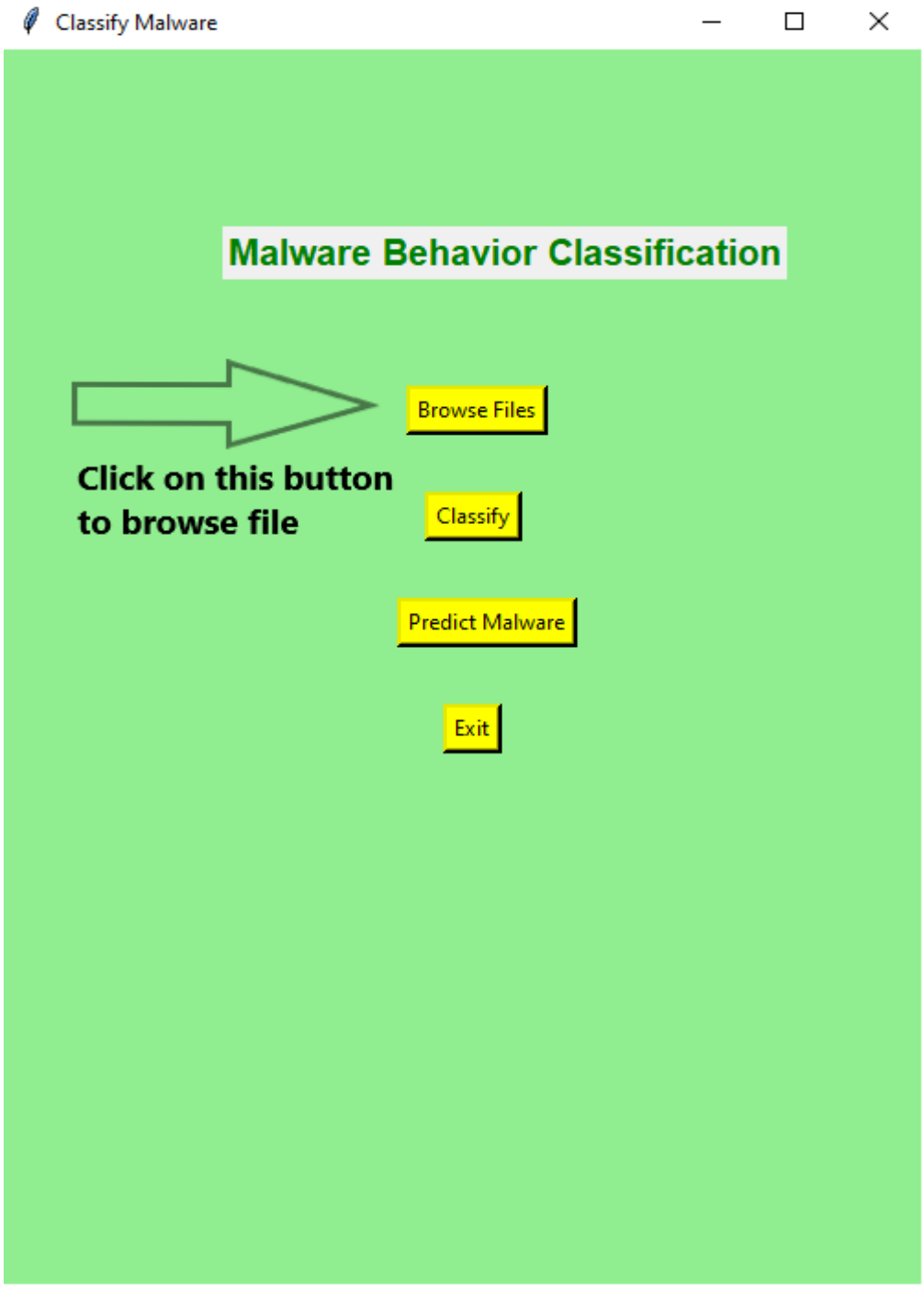
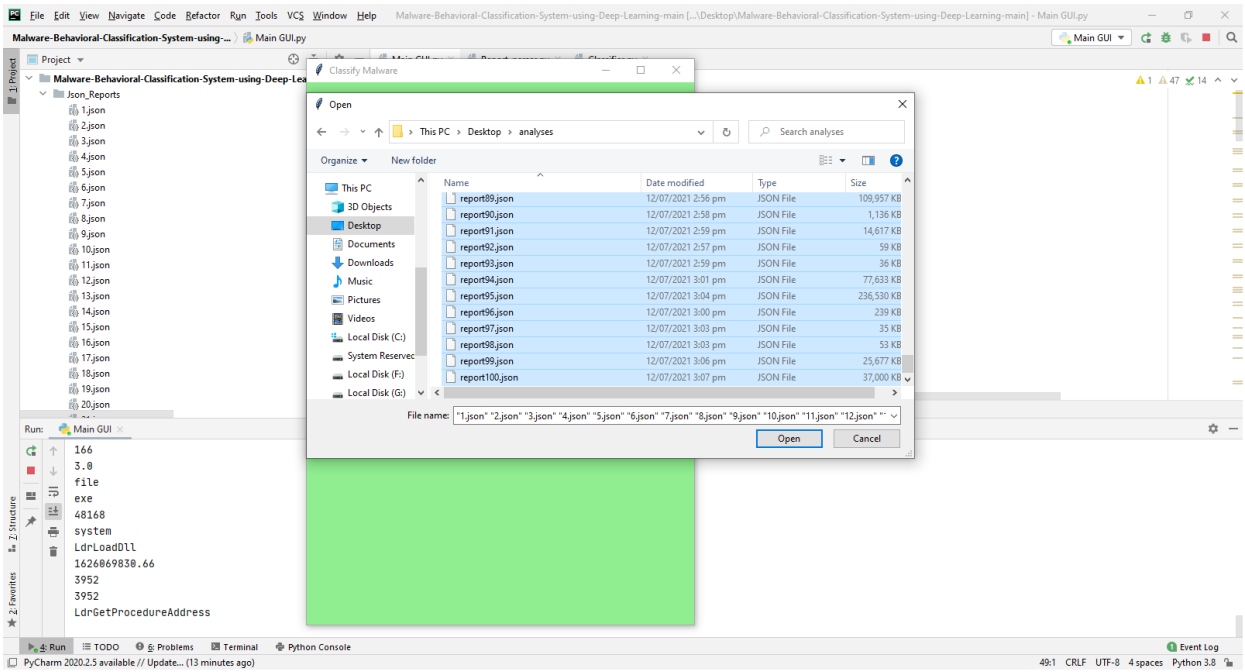


Table of Contents

Malware Classification-Select Reports

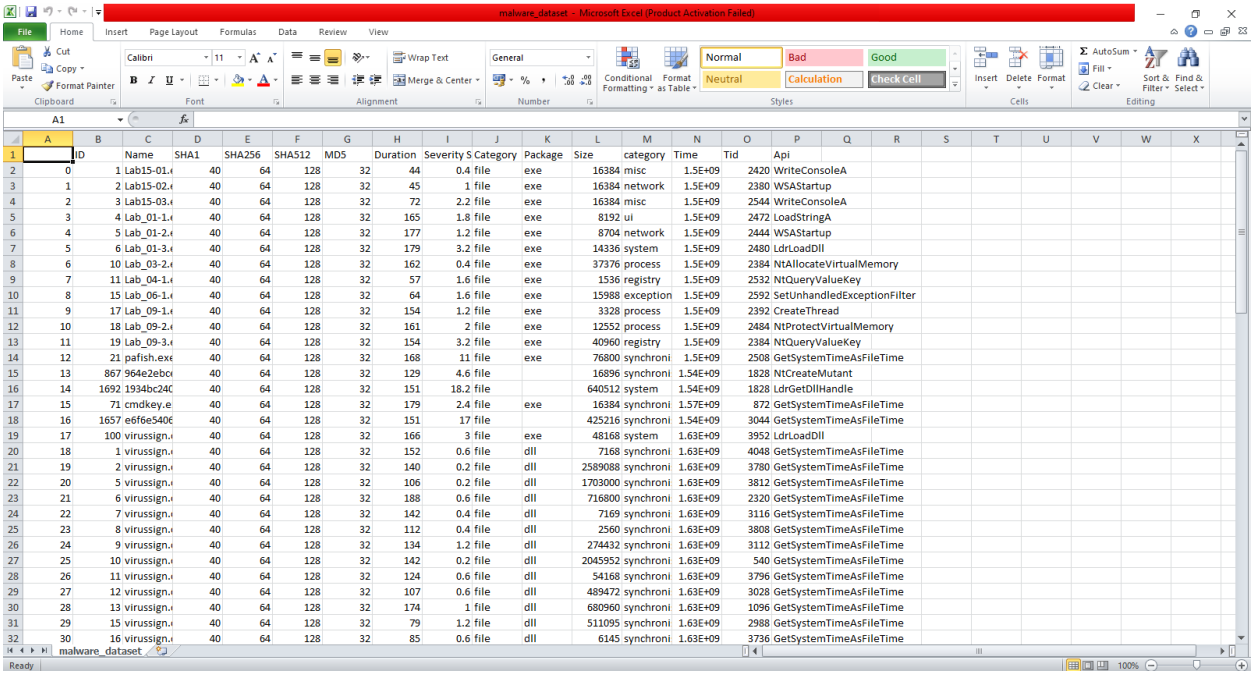
- **The user will select malware analysis report in JSON form.**
- **Based on these JSON files system will extract features.**





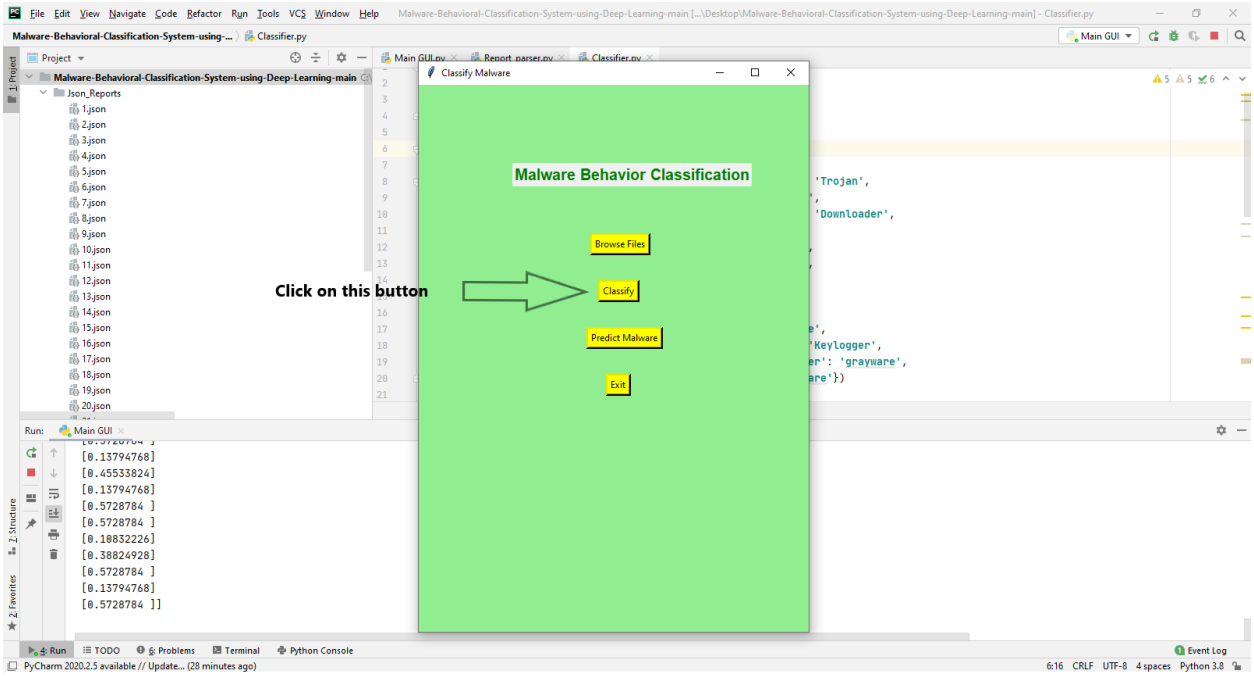
Malware Classification-Extract Features

- **The Extracted features are saved in CSV format show in figure below.**



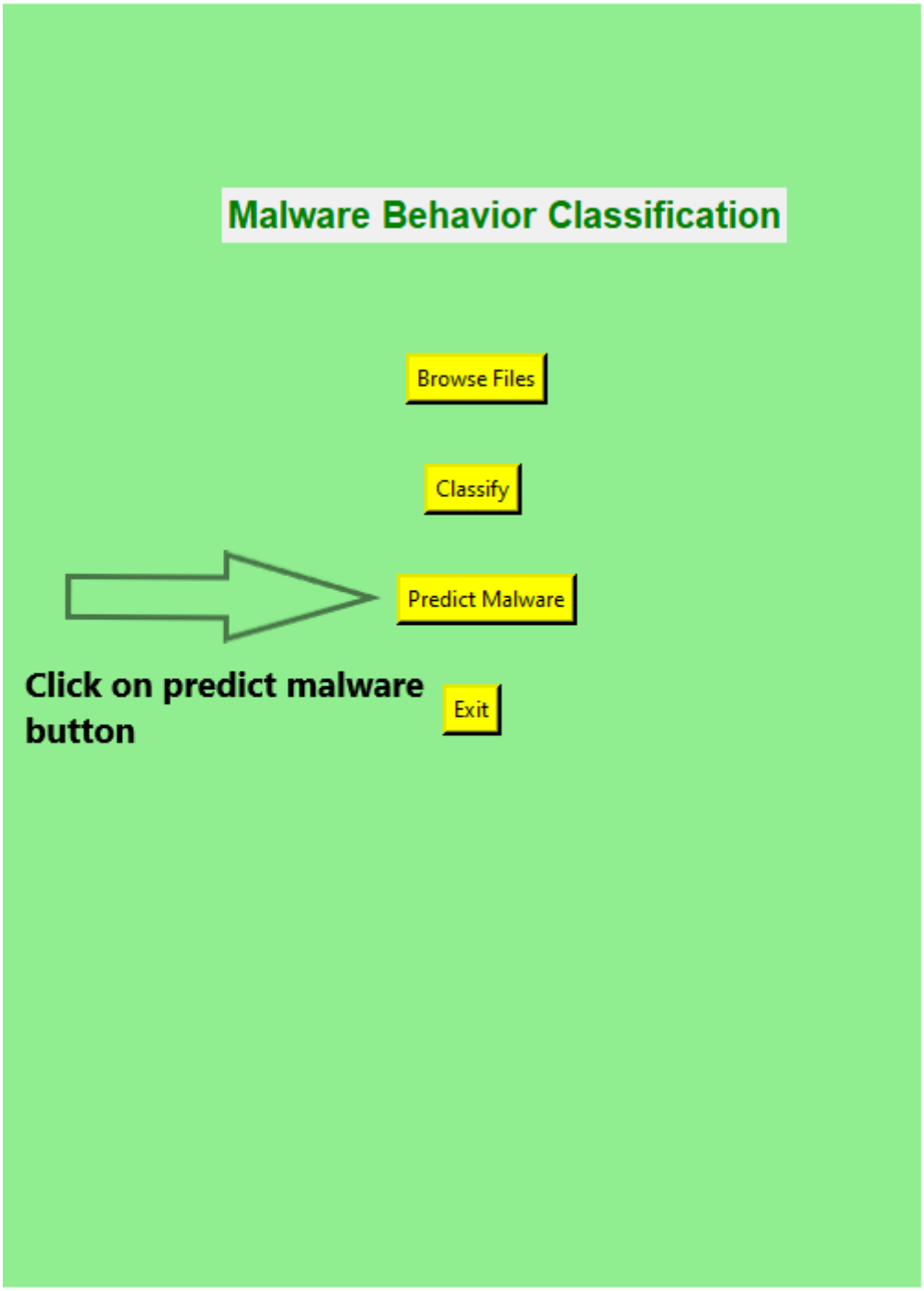
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1		ID	Name	SHA1	SHA256	SHA512	MD5	Duration	Severity S	Category	Package	Size	category	Time	Tid	Api
2		0	1	Lab15-01.(	40	64	128	32	44	0.4	file	exe	16384	misc	1.5E+09	2420	WriteConsoleA
3		1	2	Lab15-02.(	40	64	128	32	45	1	file	exe	16384	network	1.5E+09	2380	WSAStartup
4		2	3	Lab15-03.(	40	64	128	32	72	2.2	file	exe	16384	misc	1.5E+09	2544	WriteConsoleA
5		3	4	Lab_01-1.(	40	64	128	32	165	1.8	file	exe	8192	ui	1.5E+09	2472	LoadStringA
6		4	5	Lab_01-2.(	40	64	128	32	177	1.2	file	exe	8704	network	1.5E+09	2444	WSAStartup
7		5	6	Lab_01-3.(	40	64	128	32	179	3.2	file	exe	14336	system	1.5E+09	2480	LdrLoadDll
8		6	10	Lab_03-2.(	40	64	128	32	162	0.4	file	exe	37376	process	1.5E+09	2384	NtAllocateVirtualMemory
9		7	11	Lab_04-1.(	40	64	128	32	57	1.6	file	exe	1536	registry	1.5E+09	2532	NtQueryValueKey
10		8	15	Lab_06-1.(	40	64	128	32	64	1.6	file	exe	15988	exception	1.5E+09	2592	SetUnhandledExceptionFilter
11		9	17	Lab_09-1.(	40	64	128	32	154	1.2	file	exe	3328	process	1.5E+09	2392	CreateThread
12		10	18	Lab_09-2.(	40	64	128	32	161	2	file	exe	12552	process	1.5E+09	2484	NtProtectVirtualMemory
13		11	19	Lab_09-3.(	40	64	128	32	154	3.2	file	exe	40960	registry	1.5E+09	2384	NtQueryValueKey
14		12	21	pafish.exe	40	64	128	32	168	11	file	exe	76800	synchroni	1.5E+09	2508	GetSystemTimeAsFileTime
15		13	867	964e2ebc(	40	64	128	32	129	4.6	file		16896	synchroni	1.54E+09	1828	NtCreateMutant
16		14	1692	1934bc24(	40	64	128	32	151	18.2	file		640512	system	1.54E+09	1828	LdrGetDllHandle
17		15	71	cmdkey.e	40	64	128	32	179	2.4	file	exe	16384	synchroni	1.57E+09	872	GetSystemTimeAsFileTime
18		16	1657	e6f6e540(	40	64	128	32	151	17	file		425216	synchroni	1.54E+09	3044	GetSystemTimeAsFileTime
19		17	100	virussign.(	40	64	128	32	166	3	file	exe	48168	system	1.63E+09	3952	LdrLoadDll
20		18	1	virussign.(	40	64	128	32	152	0.6	file	dll	7168	synchroni	1.63E+09	4048	GetSystemTimeAsFileTime
21		19	2	virussign.(	40	64	128	32	140	0.2	file	dll	2589088	synchroni	1.63E+09	3780	GetSystemTimeAsFileTime
22		20	5	virussign.(	40	64	128	32	106	0.2	file	dll	1703000	synchroni	1.63E+09	3812	GetSystemTimeAsFileTime
23		21	6	virussign.(	40	64	128	32	188	0.6	file	dll	716800	synchroni	1.63E+09	2320	GetSystemTimeAsFileTime
24		22	7	virussign.(	40	64	128	32	142	0.4	file	dll	7169	synchroni	1.63E+09	3116	GetSystemTimeAsFileTime
25		23	8	virussign.(	40	64	128	32	112	0.4	file	dll	2560	synchroni	1.63E+09	3808	GetSystemTimeAsFileTime
26		24	9	virussign.(	40	64	128	32	134	1.2	file	dll	274432	synchroni	1.63E+09	3112	GetSystemTimeAsFileTime
27		25	10	virussign.(	40	64	128	32	142	0.2	file	dll	2045952	synchroni	1.63E+09	540	GetSystemTimeAsFileTime
28		26	11	virussign.(	40	64	128	32	124	0.6	file	dll	54168	synchroni	1.63E+09	3796	GetSystemTimeAsFileTime
29		27	12	virussign.(	40	64	128	32	107	0.6	file	dll	489472	synchroni	1.63E+09	3028	GetSystemTimeAsFileTime
30		28	13	virussign.(	40	64	128	32	174	1	file	dll	680960	synchroni	1.63E+09	1096	GetSystemTimeAsFileTime
31		29	15	virussign.(	40	64	128	32	79	1.2	file	dll	511095	synchroni	1.63E+09	2988	GetSystemTimeAsFileTime
32		30	16	virussign.(	40	64	128	32	85	0.6	file	dll	6145	synchroni	1.63E+09	3736	GetSystemTimeAsFileTime

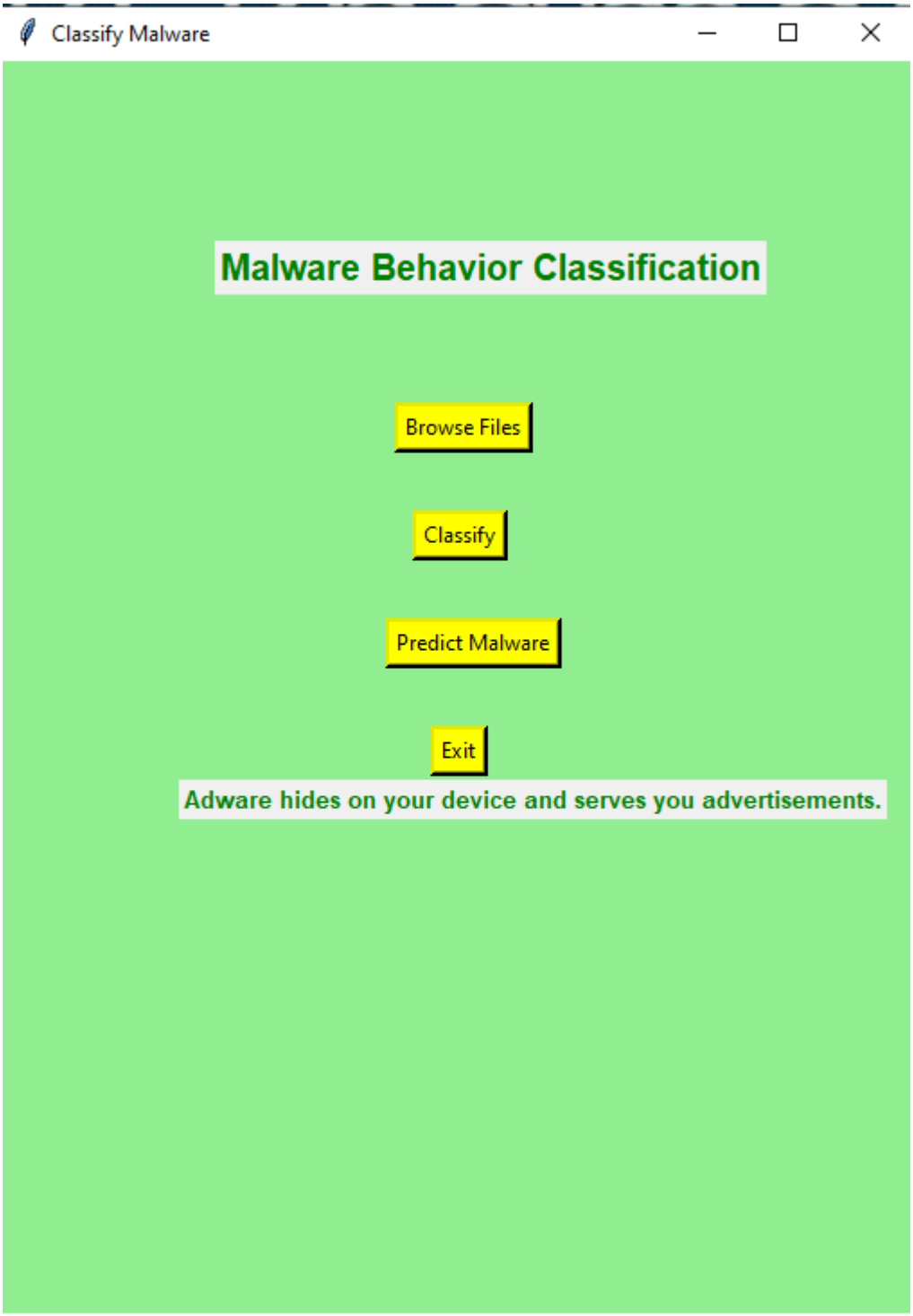
- **Then user will click classify button to perform malware classification.**
- **This classification is performed based on extracted API's.**

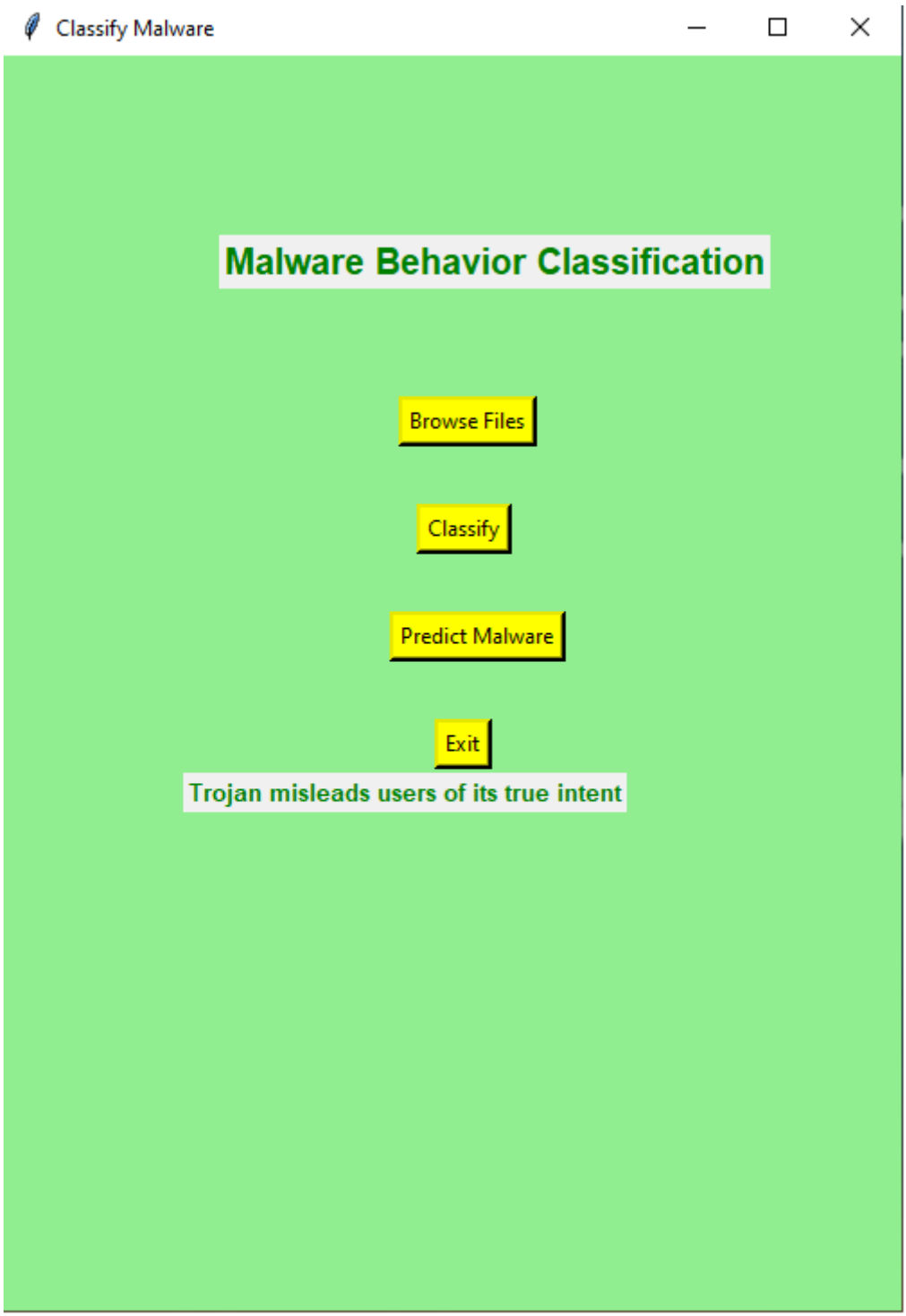


Malware Classification-Malware Prediction

- **After extracting features and performing classification now predict result.**
- **For predicting result trained model is saved in H5 file.**
- **The user clicks on predict malware button to see final output.**




Classify Malware
Malware Behavior Classification
Browse Files
Classify
Predict Malware
Exit
Adware hides on your device and serves you advertisements.


Classify Malware
Malware Behavior Classification
Browse Files
Classify
Predict Malware
Exit
Trojan misleads users of its true intent