Forensic Analysis of Android Privacy Browsing (Report)

Lab Setup:

Software	Versions
Host OS- Windows 11 Home	21H2
Oracle Virtual Box	6.1
Android X86	9.0-r2
Kali Linux (For russing analysis tools)	2022.3
Autopsy	4.19.3
Google Chrome APK	105.0.5195.79
Firefox APK	107.2.0
Firefox focus APK	107.2.0
Tor APK	102.2.1(11.5.8-Release)
Brave APK	1.45.133
Opera APK	72.2.3767.68393
Dolphin APK	12.2.9
Duckduckgo APK	5.144.0

VM Configurations:

Processors: 2
RAM: 4GB
Storage: 16GB
VM File format: Virtual Disk Image(VDI)
OS: android-x86_64-9.0-r2

Browser Test Scripts:

1) It's expected the required browser is running in VM
2) The Browser is expected to be in privacy(Incognito) mode while running scripts
3) The following search string is browsed on each separate tab with respect to corresponding search engine

Search Engine	Search String
google.com	Content_search_research_test
google.com	Convict_search_research_test
yahoo.com	Symptom_search_research_test
yahoo.com	Deprive_search_research_test
youtube.com	Nightmare_search_research_test
youtube.com	Flood_search_research_test
youtube.com	Craftsman_search_research_test
bing.com	Tolerate_search_research_test
bing.com	Flow_search_research_test
bing.com	Spill_search_research_test
duckduckgo.com	Intrusion_search_research_test
duckduckgo.com	Infiltrate_search_research_test
yandex.com	Conclude_search_research_test
yandex.com	Confirm_search_research_test

4) The following sites are visited and then bookmarked

Websites
yahoo.com
twitter.com
nytimes.com
2700chess.com
wikipedia.org
uselessweb.com
reddit.com
youtube.com

5) We sent emails from protonmail to gmail, yahoo to gmail and from gmail to yahoo and read all the emails to stimulate email activity using browser

6) User accounts are as follows :

Website	User Account
www.gmail.com	sumithtest97@gmail.com
www.yahoo.com	sumithtest97@yahoo.com
www.protonmail.com	joepandarocks@protonmail.com

7) The content sent in the emails are as follows :

From	Destination	Subject	Body
sumithtest97@gmail.com	sumithtest97@yahoo.com	Private2_email_research_test	This is a research email sent from gmail to yahoo keyword:Private2_email_research_test
sumithtest97@yahoo.com	sumithtest97@gmail.com	Continental2_email_research_test	This is a research email sent from yahoo to gmail keyword:Continental2_email_research_test
joepandarocks@protonmail.com	sumithtest97@gmail.com	Anonymous2_email_research_test	This is a research email sent from protonmail to gmail keyword:Anonymous2_email_research_test

8) After running the above mentioned script, ensure to close down all the tabs and in the case of duckduckgo click on the fire button to remove all the data. Then close the browser application.
9) Shutdown the Virtual Machine

Data Extraction and Population :

1) Use FTK Imager tool to create EnCase Image file (.E01) using Virtual Machine's Virtual Disk Image (VDI)
2) This EnCase Image file generated by FTK Imager is used by Autopsy and Bulk Extractor for Analysis
3) Bulk Extractor differentiates itself from other forensic tools by probing every byte of data and recursively extract structured data into a specific directory.
   Command to generate output directory
   Bulk_extarctor -o output_directory target_image
4) Here the output_directory is the path where our results are stored and target_image is Encase image file

5) Below are the following statistics used for comparison across test Virtual Machines after completing the test script

Bulk_extractor Feature File	Description
Domain_Histogram.txt	domains visited on the VM and the number of times each was visited
Domain.txt	domains found on the VM, including dotted-quad addresses found in text
email_domain_histogram.txt	email domains used on the VM, and the number of times each was used
email_histogram.txt	email addresses used on the VM, and the number of times each was used
email.txt	email addresses used on the VM
json.txt	JSON file structures identified on the VM
url_searches.txt	histogram of terms used in Internet searches from services
url_services.txt	histogram of the domain name portion of all the URLs found on the VM.
sqlite_carved	directory of extracted sqlite.db structures
url_histogram.txt	URLs, typically found in browser caches, email messages, and pre-compiled into executables and the number of times each was used.
url.txt	URLs, typically found in browser caches, email messages, and pre-compiled into executables.

6) Sample of output directory of bulk extractor

7) After generating this output directory we use this as an input to Browser_Excel_Generate.py file . This program outputs the total no. of artifacts in each feature file for a particular search string.The python script makes use of linux grep command to recursively parse the output directory and generate statistics for comparison across the test Virtual Machines.
8) The command is (grep -a -R search_string output_directory | cut -d :-f 1 | grep feature_file | sort -d |wc -l) .Search_string is the string which we want to search. The output of this commands gives us total no. of artifacts found in the particular feature_file

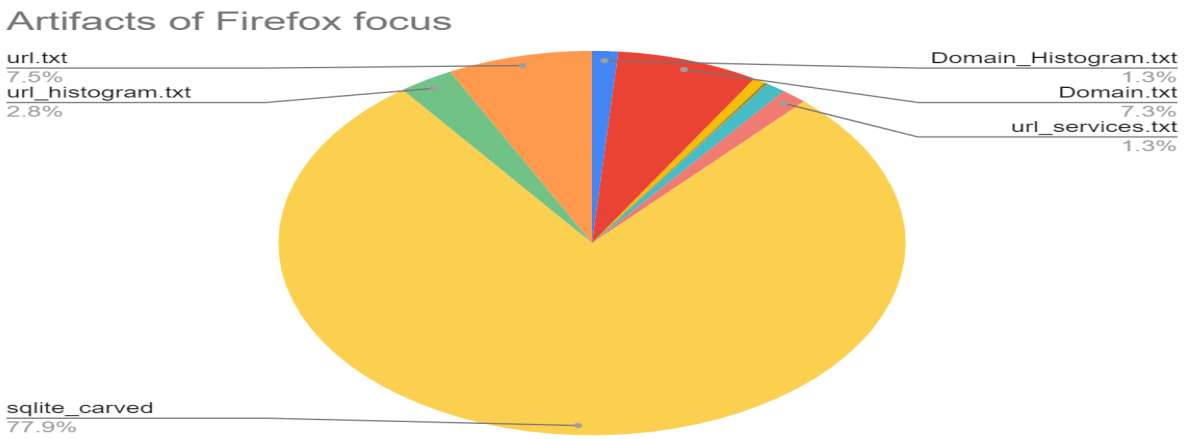
Analysis and Findings :

1) For Base VM these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_artifacts
Base VM	yahoo.com	0	0	0	0	0	0	0	0	0	0	0	0
	twitter.com	0	0	0	0	0	0	0	0	0	0	0	0
	nytimes.com	0	0	0	0	0	0	0	0	0	0	0	0
	2700chess.com	0	0	0	0	0	0	0	0	0	0	0	0
	wikipedia.org	0	0	0	0	0	0	0	0	0	0	0	0
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	0	0	0	0	0	0	0	0	0	0	0	0
	duckduckgo.com	0	0	0	0	0	0	0	0	0	0	0	0
	yandex.com	0	0	0	0	0	0	0	0	0	0	0	0
	bing.com	0	0	0	0	0	0	0	0	0	0	0	0
	youtube.com	1	4	0	0	0	0	0	0	17	2	4	28
	anonymous2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0	0	0	0	0	28

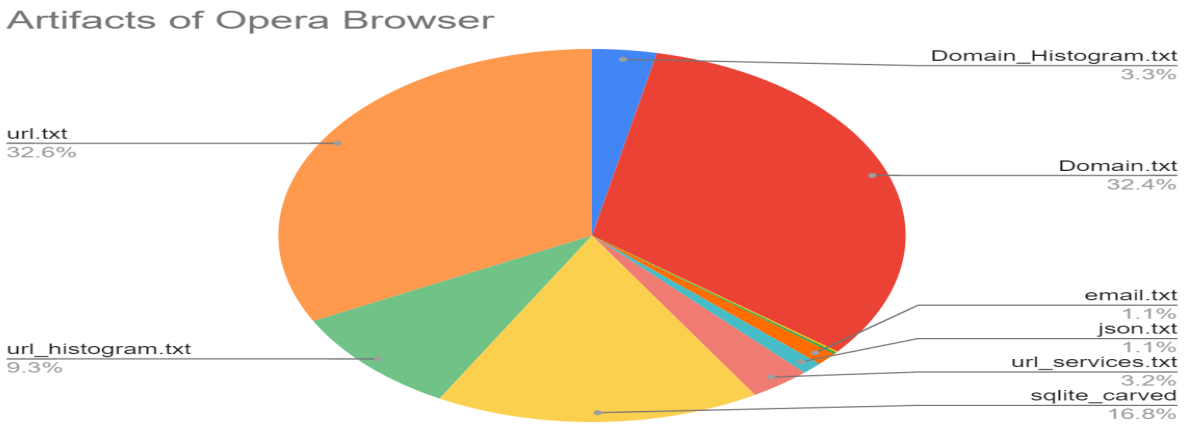
2) For Firefox focus browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_artifacts
Firefox focus	yahoo.com	3	17	0	0	0	6	0	3	252	6	18	305
	twitter.com	1	3	0	0	0	0	0	1	0	1	3	9
	nytimes.com	1	2	0	0		0	0	1	0	1	2	7
	2700chess.com	1	1	0	0	0	0	0	1	0	1	1	5
	wikipedia.org	3	20	7	0	0	0	0	3	296	5	20	354
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	0	0	0	0	0	0	0	0	0	0	0	0
	duckduckgo.com	1	3	0	0	0	0	0	1	3	3	3	14
	yandex.com	0	0	0	0	0	0	0	0	0	0	0	0
	bing.com	1	4	0	0	0	0	0	1	3	4	4	17
	youtube.com	6	43	1	1	1	7	0	6	435	15	44	559
	anonymous2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	17	93	8	1	1	13	0	17	989	36	95	1270



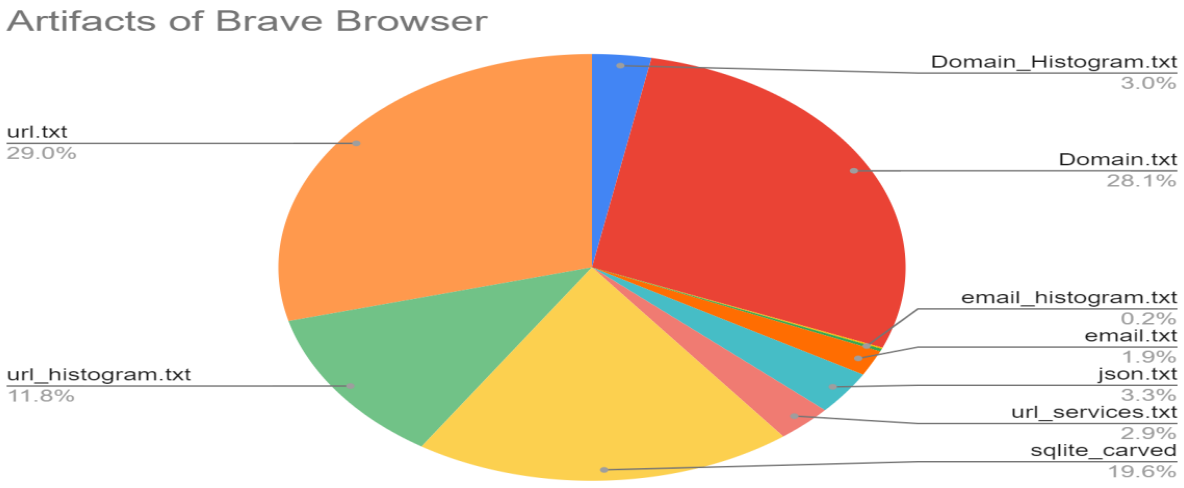
3) For Opera Browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_Artifacts
Opera Browser	yahoo.com	36	430	1	2	18	9	0	34	78	96	412	1116
	twitter.com	7	25	1	1	2	0	0	6	42	29	43	156
	nytimes.com	0	0	0	0	0	0	0	0	0	0	0	0
	2700chess.com	0	0	0	0	0	0	0	0	0	0	0	0
	wikipedia.org	1	4	0	0	0	0	0	1	1	3	4	14
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	0	0	0	0	0	0	0	0	0	0	0	0
	duckduckgo.com	1	22	0	0	0	0	0	1	3	5	22	54
	yandex.com	5	34	0	0	0	0	0	5	0	8	35	87
	bing.com	1	29	0	0	0	0	0	1	3	7	29	70
	youtube.com	8	31	0	0	0	4	0	8	116	18	34	219
	anonymous2_email_research_test	0	0	0	0	0	6	0	0	55	0	0	61
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	59	575	2	3	20	19	0	56	296	166	579	1777



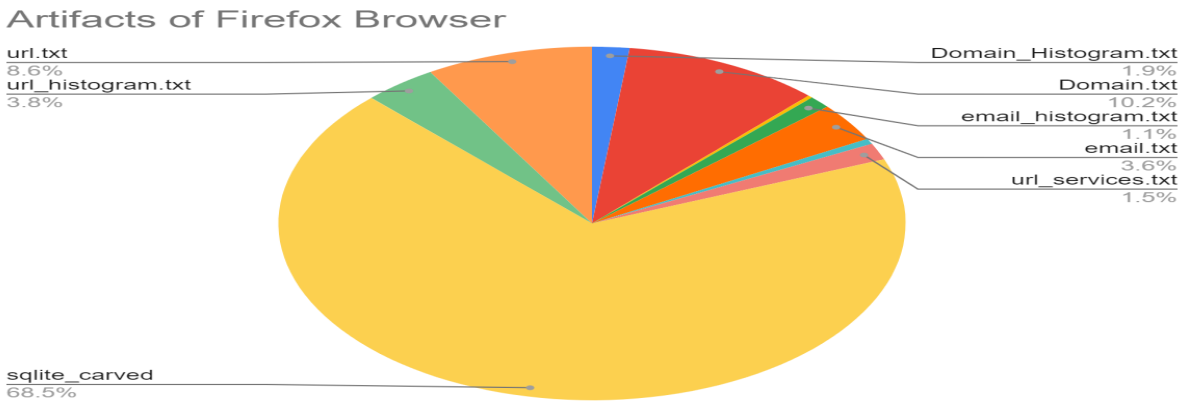
4) For Brave browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_artifacts
Brave Browser	yahoo.com	36	315	1	2	33	20	0	34	74	97	284	896
	twitter.com	7	100	1	2	6	5	0	6	36	80	132	375
	nytimes.com	0	0	0	0	0	0	0	0	0	0		0
	2700chess.com	0	0	0	0	0	0	0	0	0	0	0	0
	wikipedia.org	1	3	0	0	0	0	0	1	0	2	5	12
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	0	0	0	0	0	4	0	0	12	0	0	16
	duckduckgo.com	2	20	0	0	0	0	0	2	6	7	20	57
	yandex.com	6	27	0	0	0	5	0	6	24	11	29	108
	bing.com	1	32	0	0	0	5	0	1	18	10	36	103
	youtube.com	8	67	0	0	0	8	0	8	91	30	77	289
	anonymous2_email_research_test	0	0	0	0	0	19	0	0	132	0	0	151
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	61	564	2	4	39	66	0	58	393	237	583	2007



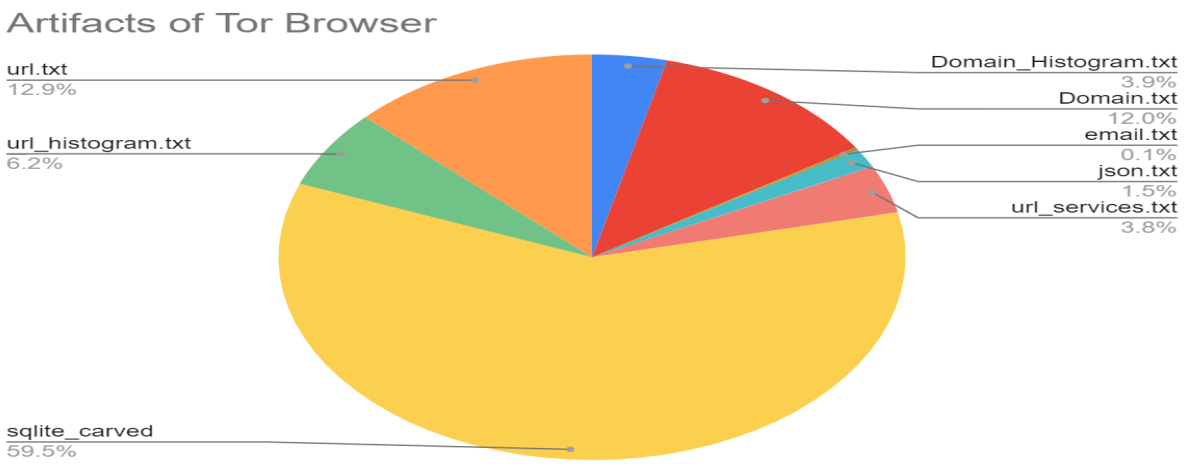
5) For Firefox browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_artifacts
Fire Fox Browser	yahoo.com	10	41	2	6	30	0	0	6	262	7	20	384
	twitter.com	6	65	1	15	40	0	0	5	292	6	34	464
	nytimes.com	3	18	0	0	0	1	0	3	59	11	18	113
	2700chess.com	2	9	0	0	0	2	0	2	77	6	9	107
	wikipedia.org	4	20	0	0	0	2	0	4	63	12	20	125
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	4	10	0	0	0	4	0	4	49	5	12	88
	duckduckgo.com	1	1	0	0	0	0	0	1	0	1		4
	yandex.com	0	0	0	0	0	0	0	0	0	0	0	0
	bing.com	0	0	0	0	0	0	0	0	0	0	0	0
	youtube.com	9	43	2	2	2	1	0	6	571	29	62	727
	anonymous2_email_research_test	0	0	0	0	0	0	0	0	16	0	0	16
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	39	207	5	23	72	10	0	31	1389	77	175	2028



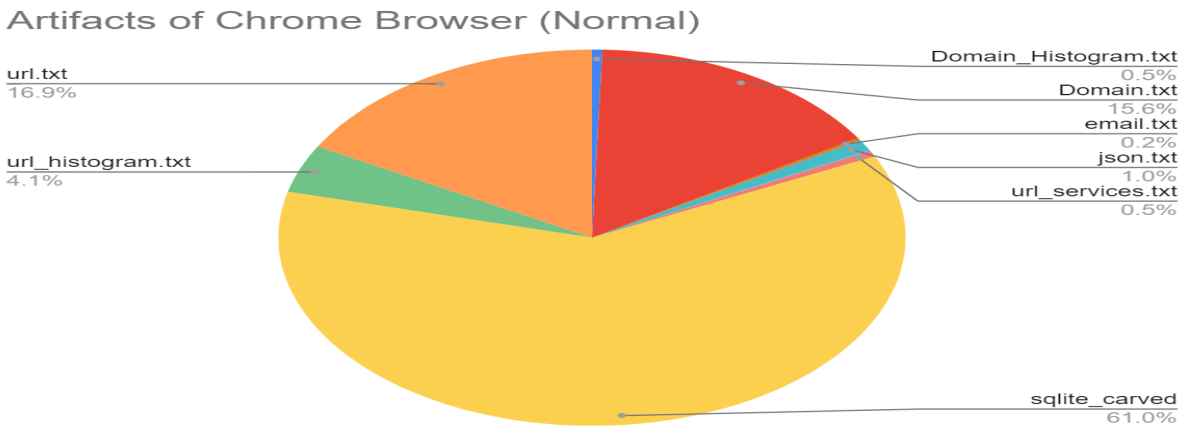
6) For Tor browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_Histogram.txt	url.txt	Total_artifacts
Tor Browser	yahoo.com	59	89	0	0	0	9	1	59	281	69	91	658
	twitter.com	4	22	0	0	0	2	0	4	220	5	34	291
	nytimes.com	2	3	0	0	0	0	0	2	0	2	3	12
	2700chess.com	0	0	0	0	0	0	0	0	0	0	0	0
	wikipedia.org	6	51	0	0	0	11	0	6	304	27	51	456
	uselessweb.com	0	0	0	0	0	0	0	0	0	0	0	0
	reddit.com	2	4	0	0	0	1	0	2	0	3	5	17
	duckduckgo.com	3	43	0	0	0	1	0	3	15	8	44	117
	yandex.com	8	9	0	0	0	0	0	8	0	8	9	42
	bing.com	2	11	0	0	0	1	0	2	31	7	11	65
	youtube.com	8	62	1	1	2	12	0	7	600	23	66	782
	anonymous2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Confirm_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Total	94	294	1	1	2	37	1	93	1451	152	314	2440



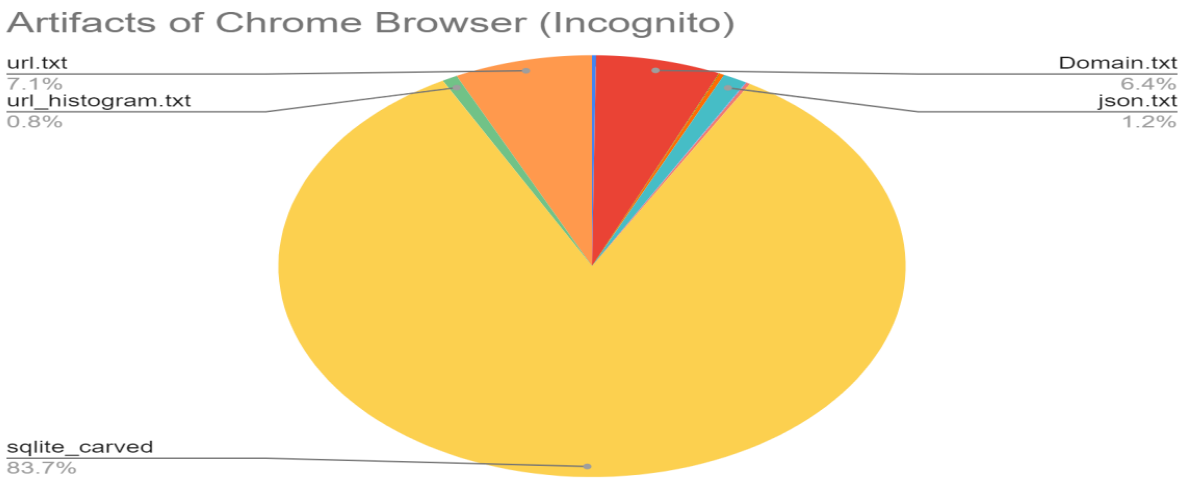
7) For Chrome Browser in normal mode these are following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_Histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_Artifacts
Chrome Browser (Normal)	yahoo.com	60	3121	1	4	10	128	16	59	13535	803	3791	21528
	twitter.com	34	4804	0	0	0	137	3	34	9497	739	4895	20143
	nytimes.com	49	3134	1	11	144	118	5	48	5979	1100	3102	13691
	2700chess.com	2	378	0	0	0	62	3	2	4618	119	418	5602
	wikipedia.org	300	964	0	0	0	108	0	300	6723	372	979	9746
	uselessweb.com	4	229	1	1	1	57	1	3	3730	30	236	4293
	reddit.com	7	561	0	0	0	143	0	7	4791	138	592	6239
	duckduckgo.com	4	220	0	0	0	6	0	4	160	66	220	680
	yandex.com	14	134	0	0	0	4	0	14	33	73	136	408
	bing.com	3	150	0	0	0	14	0	3	978	42	177	1367
	youtube.com	8	649	0	0	0	117	3	8	4161	173	681	5800
	anonymous2_email_research_test	0	0	0	0	0	11	0	0	271	0	0	282
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	1	0	309	11	53	374
	Convict_search_research_test	0	0	0	0	0	0	1	0	186	3	19	209
	Symptom_search_research_test	0	0	0	0	0	0	4	0	193	4	27	228
	Deprive_search_research_test	0	0	0	0	0	1	4	0	203	7	7	222
	Nightmare_search_research_test	0	0	0	0	0	1	0	0	181	8	25	215
	Flood_search_research_test	0	0	0	0	0	1	0	0	152	9	25	187
	Craftsman_search_research_test	0	0	0	0	0	1	0	0	177	4	22	204
	Tolerate_search_research_test	0	0	0	0	0	0	1	0	50	5	14	70
	Flow_search_research_test	0	0	0	0	0	0	1	0	47	3	10	61
	Spill_search_research_test	0	0	0	0	0	0	1	0	47	3	7	58
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	72	4	8	84
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	30	14	46	90
	Conclude_search_research_test	0	0	0	0	0	0	6	0	0	31	48	85
	Confirm_search_research_test	0	0	0	0	0	0	6	0	4	30	47	87
	Total	485	14344	3	16	155	909	56	482	56127	3791	15585	91953



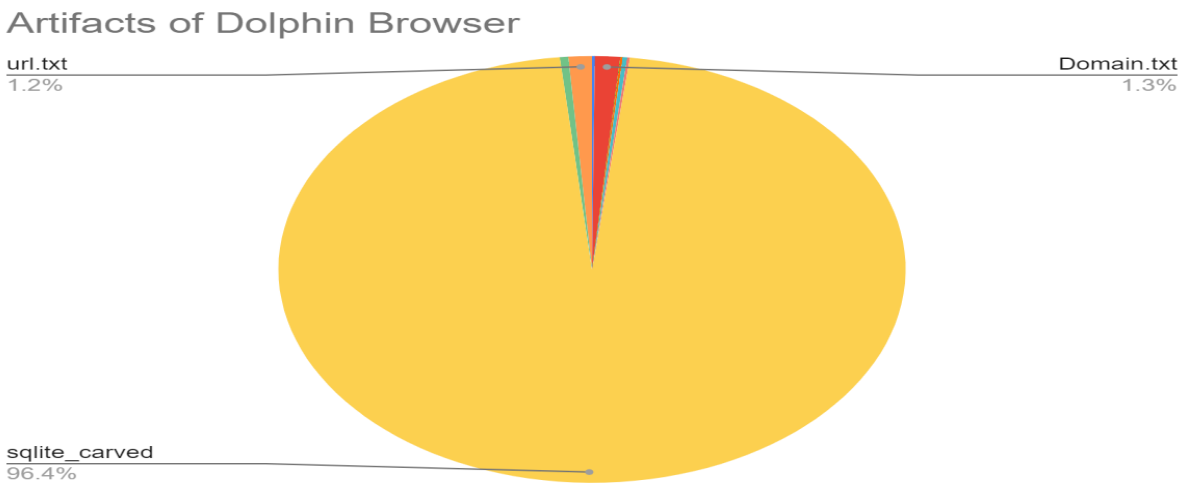
8) For Chrome Browser in Incognito mode these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_Histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_Artifacts
Chrome Browser (Incognito Final)	yahoo.com	7	214	1	2	36	70	1	5	3621	17	183	4157
	twitter.com	8	155	1	1	4	5	0	7	1747	33	191	2152
	nytimes.com	1	66	0	0	0	4	0	1	776	1	66	915
	2700chess.com	1	63	0	0	0	3	0	1	813	2	63	946
	wikipedia.org	3	148	0	0	0	43	0	3	1664	6	148	2015
	uselessweb.com	1	50	0	0	0	0	0	1	525	1	50	628
	reddit.com	2	48	0	0	0	0	0	2	466	2	48	568
	duckduckgo.com	1	37	0	0	0	0	0	1	170	9	37	255
	yandex.com	1	20	0	0	0	0	0	1	108	3	20	153
	bing.com	1	56	0	0	0	0	0	1	330	9	56	453
	youtube.com	7	171	0	0	0	42	0	7	1959	26	177	2389
	anonymous2_email_research_test	0	0	0	0	0	31	0	0	449	0	0	480
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	1	0	6	2	3	12
	Convict_search_research_test	0	0	0	0	0	0	1	0	88	1	12	102
	Symptom_search_research_test	0	0	0	0	0	0	1	0	45	1	1	48
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	29	2	2	33
	Flood_search_research_test	0	0	0	0	0	0	0	0	28	2	2	32
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	82	1	4	87
	Tolerate_search_research_test	0	0	0	0		0	1	0	2	1	1	5
	Flow_search_research_test	0	0	0	0	0	0	1	0	26	1	1	29
	Spill_search_research_test	0	0	0	0	0	0	1	0	174	1	28	204
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	2	1	1	4
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	162	1	23	186
	Conclude_search_research_test	0	0	0	0	0	0	0	0	2	1	1	4
	Confirm_search_research_test	0	0	0	0	0	0	0	0	104	1	18	123
	Total	33	1028	2	3	40	198	7	30	13378	125	1136	15980



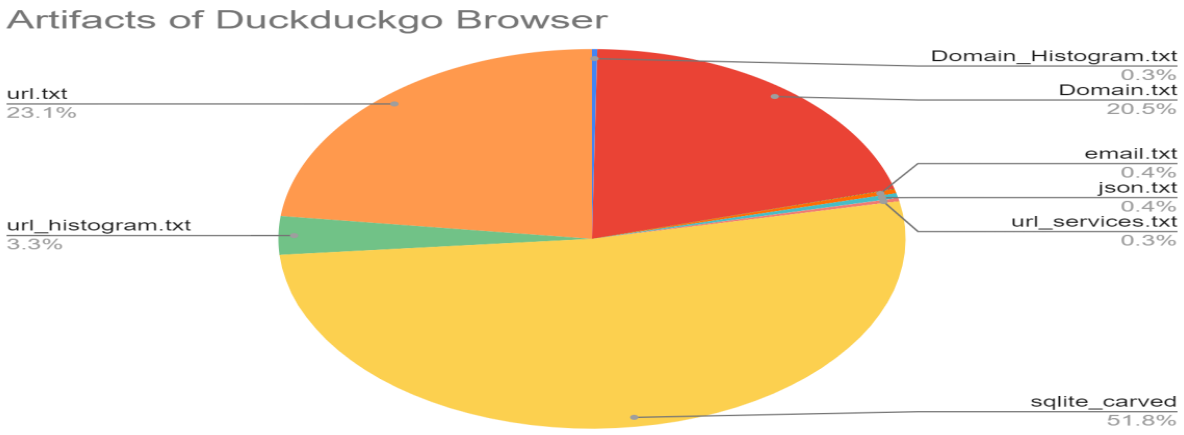
9) For Dolphin Browser these are the following statistics

Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_Artifacts
Dolphin	yahoo.com	14	100	1	3	31	33	0	12	1741	21	24	1960
	twitter.com	9	77	1	1	4	2	0	8	3607	48	109	3866
	nytimes.com	8	55	0	0	0	1	0	8	3326	18	55	3471
	2700chess.com	1	4	0	0	0	0	0	1	2430	1	4	2441
	wikipedia.org	3	47	0	0	0	16	0	3	2420	11	47	2547
	uselessweb.com	0	0	0	0	0	0	0	0	1943	0	0	1943
	reddit.com	1	17	0	0	0	1	0	1	2822	4	20	2866
	duckduckgo.com	1	5	0	0	0	1	0	1	26	4	5	43
	yandex.com	1	30	0	0	0	1	0	1	2353	2	31	2419
	bing.com	2	15	0	0	0	2	0	2	2337	7	17	2382
	youtube.com	9	88	0	0	0	17	0	9	8491	31	96	8741
	anonymous2_email_research_test	0	0	0	0	0	5	0	0	123	0	0	128
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Convict_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Symptom_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Deprive_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Nightmare_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flood_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Craftsman_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Tolerate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Flow_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Spill_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Intrusion_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Infiltrate_search_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Conclude_search_research_test	0	0	0	0	0	0	0	0	97	0	0	97
	Confirm_search_research_test	0	0	0	0	0	0	0	0	833	0	0	833
	Total	49	438	2	4	35	79	0	46	32549	147	408	33757



10) For Duckduckgo browser these are the following statistics

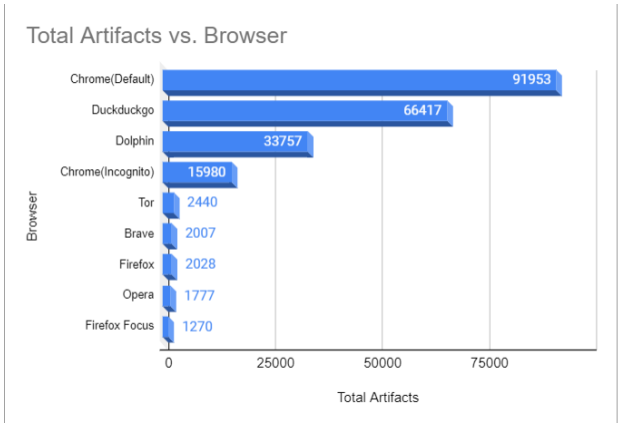
Browser	Search Term	Domain_Histogram.txt	Domain.txt	email_domain_histogram.txt	email_histogram.txt	email.txt	json.txt	url_searches.txt	url_services.txt	sqlite.db	url_histogram.txt	url.txt	Total_artifacts
Duckduckgo	yahoo.com	60	1733	0	0	0	30	1	60	5419	364	1859	9526
	twitter.com	32	2351	0	0	0	30	0	32	3188	227	2371	8231
	nytimes.com	42	5054	1	12	237	27	0	41	3586	901	4925	14826
	2700chess.com	2	550	0	0	0	1	0	2	2064	49	551	3219
	wikipedia.org	4	552	0	0	0	11	0	4	2636	22	552	3781
	uselessweb.com	1	2	0	0	0	0	0	1	0	2	2	8
	reddit.com	5	641	0	0	0	102	0	5	2105	13	643	3514
	duckduckgo.com	13	880	1	1	1	5	0	12	1651	119	1290	3973
	yandex.com	7	547	0	0	0	8	0	7	1928	70	551	3118
	bing.com	6	605	0	0	0	11	0	6	2856	226	605	4315
	youtube.com	8	686	0	0	0	29	0	8	3371	76	691	4869
	anonymous2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	continental2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	private2_email_research_test	0	0	0	0	0	0	0	0	0	0	0	0
	Content_search_research_test	0	0	0	0	0	0	2	0	63	16	26	107
	Convict_search_research_test	0	0	0	0	0	0	1	0	21	9	15	46
	Symptom_search_research_test	0	0	0	0	0	1	1	0	23	7	17	49
	Deprive_search_research_test	0	0	0	0	0	1	0	0	9	1	1	12
	Nightmare_search_research_test	0	0	0	0	0	2	0	0	102	2	23	129
	Flood_search_research_test	0	0	0	0	0	1	0	0	107	2	22	132
	Craftsman_search_research_test	0	0	0	0	0	1	0	0	1403	1	297	1702
	Tolerate_search_research_test	0	0	0	0	0	1	1	0	6	1	2	11
	Flow_search_research_test	0	0	0	0	0	0	1	0	22	3	6	32
	Spill_search_research_test	0	0	0	0	0	1	1	0	1329	2	282	1615
	Intrusion_search_research_test	0	0	0	0	0	2	0	0	13	6	8	29
	Infiltrate_search_research_test	0	0	0	0	0	1	0	0	1303	6	281	1591
	Conclude_search_research_test	0	0	0	0	0	2	0	0	643	23	147	815
	Confirm_search_research_test	0	0	0	0	0	2	0	0	582	21	162	767
	Total	180	13601	2	13	238	269	8	176	34430	2169	15329	66417

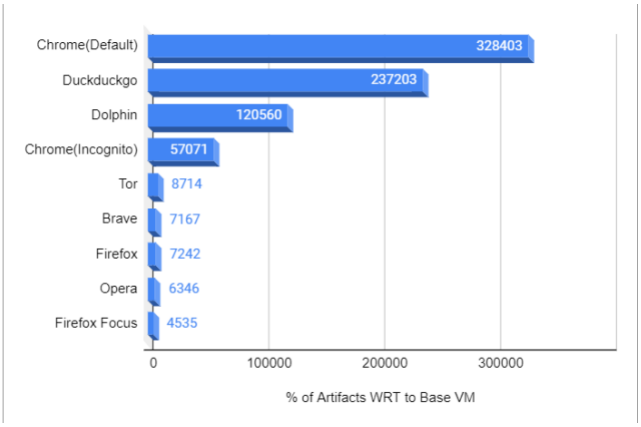


Combined statistics of Total Artifacts and %of Artifacts WRT to base VM for each browser

Browser	Total Artifacts	% of Artifacts WRT to Base VM
Chrome(Default)	91953	328403
Duckduckgo	66417	237203
Dolphin	33757	120560
Chrome(Incognito)	15980	57071
Tor	2440	8714
Brave	2007	7167
Firefox	2028	7242
Opera	1777	6346
Firefox Focus	1270	4535

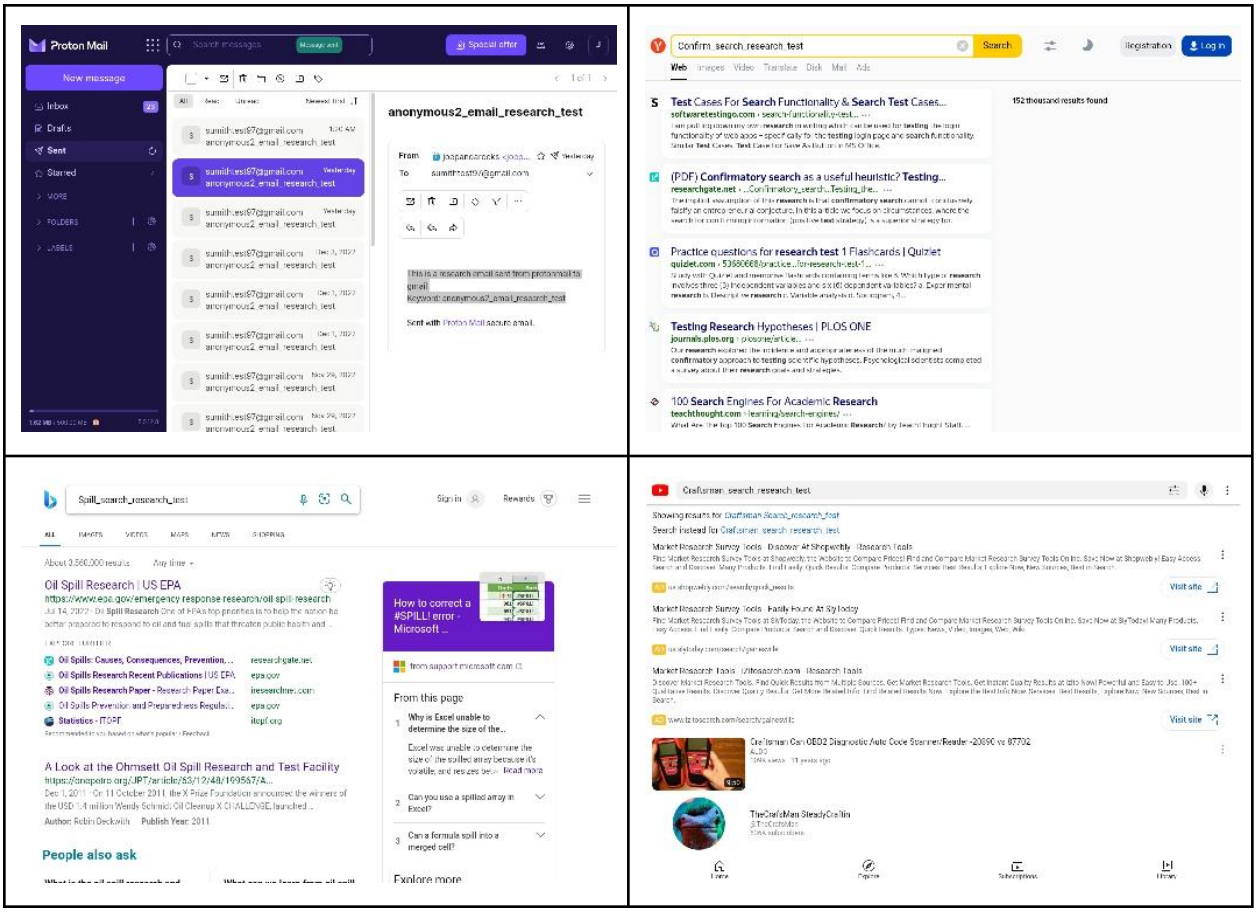
(Total Artifacts vs Browser) and (% of Artifacts WRT to Base VM vs Browser)





Autopsy Analysis Results:

For Duckduckgo was able to retrieve screenshots of browsing activities from unallocated spaces i.e was able to retrieve deleted data by the browser.



In Chrome Incognito was able to retrieve email content

84e08e71345f5b3184e08e71345f5b3false
ontinential2_email_research_testThis is a research email sent from yahoo to gmail keyword: continential2_email_research_test[null,"sumithtest97@yahoo.com","sumith g",null][[null,"sumithtest97@gmail.com","sumithtest97@gmail.com",null]]]]]
8[[null,1," <div style=\"font-family:Helvetica Neue,Helvetica,Arial,sans-serif;font-size:16px\"> <div dir=\"ltr\" style=\"font-family:Helvetica,Arial,sans-serif;font-size:18px\">This is a research email sent from yahoo to gmail
 <div dir=\"ltr\"
tyle=\"font-family:Helvetica,Arial,sans-serif;font-size:18px\">keyword: continential2_email_research_<wbr>test "]]]]2022-12-05 04:34:24
84e03b0de08bc2d)

Meta Data:

Metadata

Name:	/img_Chrome_Incognito_Final.E01/vol_vol2//$Unalloc/Unalloc_8526_71601664_2046852608
Type:	Unallocated Blocks
MIME Type:	application/octet-stream
Size:	524300288
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	8527

Results and Conclusions:

1) The analysis on normal browsing mode resulted in a lot of artifacts as expected. Since Normal mode stores all of the data including browser history, cookies, bookmarks and login details this was an expected result. Chrome incognito, though performed better than normal mode , produced lots of artifacts.

2) Autopsy results showed the existence of all test URLs in the unallocated space. Firefox private browsing performed way better than both the modes of Chrome, retaining only a small number of artifacts relatively. It only stores bookmarks which the user wants to save. Tor browser's case was very similar to Firefox as it generated the same number of artifacts approximately. Data from bookmarks were found as expected. Autopsy also revealed the bookmarks artifacts being in the same path folder as Firefox

3) The case of DuckDuckGo was a surprise as it produced way more artifacts than expected. Though it did not retain artifacts for most of the search strings except for a few, it did have artifacts from all the websites visited. Autopsy revealed the existence of images which are screenshots of browsing sessions. Nonetheless, it was carved out of unallocated space indicating DuckDuckGo deleted those files.

4) Firefox focus had the best performance out of all the browsers tested with the least number of residual artifacts generated. Opera and Brave browsers also fared very well close to the performance of Firefox. They also stored bookmark artifacts and resulted in almost none related to the search strings of our browser script. Dolphin's private browser in turn generated a lot of artifacts close to about 40% of Chrome's normal browsing mode.

5) All of the browsers generated persistent file-system based artifacts.

6) Firefox Focus performed the best out of all the tested browsers with the least number of artifacts. It is also very lightweight to use.

7) Firefox, Tor, Brave and Opera fared well too. Since Tor offers multi-nodal traffic routing , it also offers anonymity so both Focus and Tor browsers can be recommended to users with their browsing footprint concerns.

8) DuckDuckGo surprisingly generated a significant number of artifacts than expected. It also generated images of browsing sessions including email contents.

9) Any adversary with access to the Android device's disk image can uncover the browsing behavior and activities of a user putting their privacy at high risk.

Limitations of the Project:

1) It is worth noting that most of the artifacts generated are from unallocated data which requires root access to a device's disk.

2) The version used in the project is Android 9 since only this version has the most stable release for the emulator.

3) We made use of only two forensic tools which seemed like the viable option available freely.

4) The project only analyzes the most popular apps on Android while there still are numerous privacy browsers with millions of downloads