



kali@kali: ~/Desktop

File Actions Edit View Help

```
(kali@kali) - [~/Desktop]  
$ ./Analyzer.sh hdd hddfile |
```

```
(kali㉿ kali)-[~/Desktop]  
$ ./Analyzer.sh hdd hddfile  
[+] Hdd Directory created  
[+] Foremost output Directory created  
[+] Analyzing Hdd File with foremost, strings, Binwalk And Bulk_Extractor.
```



hddDirectory

mkdir "Bulk-dir"

bulk_extractor version: 2.0.0-beta2

Input file: "hddfile"

Output directory: "Bulk-dir"

Disk Size: 671094597

Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml msxml net ntf
sindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard windirs winlnk winpe winp
refetch zip accts email gps

Threads: 2

going multi-threaded...(2)

bulk_extractor Fri Sep 2 09:23:22 2022

available_memory: 5168021504

bytes_queued: 0

depth0_bytes_queued: 0

depth0_sbufs_queued: 0

elapsed_time: 0:00:00

estimated_date_completion: 2022-09-02 09:23:21

estimated_time_remaining: n/a

fraction_read: 0.000000 %

max_offset: 0

sbufs_created: 0

sbufs_queued: 0

sbufs_remaining: 0

2r?e?W=\^?T?tSθ?|/^Ff*?76.[~s?E?v]~'k?}{(H?
Ki>"?
|?????[?9?y?ur4O????w8?\Ag?\$?h?v?}W?
?yQ??W?qO?[?b/x???i??)?]k0_?[???(?a?m??=Ω?????+??
CV??=?G??0??-FY?F??\y?e?^?J7?x?????,?.ك<?W???T?B?}??°K??
??v?f;????!?????"Γ?k?[]????C?w???t?Z?{?zD[] ?`a??[?;??
?+?y.?[
*|

[*] All Data is saved at hddDirectory you are more then welcome to view them

[+] binwalk , strings and foremost log.txt was cerated successfully

Printing log.txt

Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus

Audit File

Foremost started at Fri Sep 2 09:33:27 2022

Invocation: foremost hddfile

Output directory: /home/kali/Desktop/output

Configuration file: /etc/foremost.conf

File: hddfile

Start: Fri Sep 2 09:33:27 2022

Length: 640 MB (671094597 bytes)

File Actions Edit View Help

Configuration file: /etc/foremost.conf

File: hddfile

Start: Fri Sep 2 09:33:27 2022

Length: 640 MB (671094597 bytes)

Num	Name (bs=512)	Size	File Offset	Comment
0:	00071940.gif	172 KB	36833357	(472 x 276)
1:	00221247.gif	9 B	113278642	(202 x 59)
2:	00253751.gif	2 KB	129920610	(44 x 56)
3:	00253755.gif	11 KB	129923021	(1 x 56)
4:	00254110.gif	249 KB	130104364	(108 x 100)
5:	00263981.gif	51 KB	135158762	(40 x 33)
6:	00278352.gif	151 KB	142516691	(125 x 220)
7:	00279216.gif	47 KB	142958910	(30 x 29)
8:	00279473.gif	3 KB	143090529	(190 x 157)
9:	00279497.gif	2 KB	143102701	(48 x 48)
10:	00279502.gif	2 KB	143105352	(172 x 93)
11:	00279508.gif	1 KB	143108246	(171 x 61)
12:	00279526.gif	7 KB	143117634	(170 x 204)
13:	00279549.gif	4 KB	143129420	(170 x 204)
14:	00279563.gif	3 KB	143136699	(170 x 204)
15:	00279573.gif	8 KB	143141536	(170 x 204)
16:	00279592.gif	1 KB	143151555	(170 x 204)
17:	00279608.gif	4 KB	143159530	(170 x 204)
18:	00279626.gif	3 KB	143168759	(170 x 204)
19:	00279637.gif	11 KB	143174617	(170 x 204)
20:	00279661.gif	4 KB	143186708	(170 x 204)

File	Actions	Edit	View	Help
------	---------	------	------	------

61:	01138283.gif	8 KB	582801137	(209 x 151)
62:	01138392.gif	35 KB	582856721	(265 x 176)
63:	01146078.gif	179 KB	586792260	(309 x 60)

Finish: Fri Sep 2 09:33:53 2022

64 FILES EXTRACTED

gif:= 63

zip:= 1

Foremost finished at Fri Sep 2 09:33:53 2022




DECIMAL	HEXADECIMAL	DESCRIPTION
---------	-------------	-------------

52960	0xCEE0	Zip archive data, at least v2.0 to extract, compressed size: 16746, uncompressed size: 18031, name: transport_down.jpg
546891	0x8584B	Zip archive data, at least v2.0 to extract, compressed size: 508, uncompressed size: 1414, name: goo.js
547471	0x85A8F	Zip archive data, at least v2.0 to extract, compressed size: 8135, uncompressed size: 10032, name: ffw_default.bmp
555697	0x87AB1	Zip archive data, at least v2.0 to extract, compressed size: 8035, uncompressed size: 10032, name: ffw_down.bmp
563820	0x89A6C	Zip archive data, at least v2.0 to extract, compressed size: 8531, uncompressed size: 10032, name: ffw_rollover.bmp
572449	0x8BC21	Zip archive data, at least v2.0 to extract, compressed size: 121949, uncompressed size: 245972, name: frame.bmp
11149651	0xAA2153	Microsoft Cabinet archive data, 1802240 bytes, 1 file
12878597	0xC48305	MySQL ISAM index file Version 11










size: 16044, uncompressed size: 45056, name: pwservice.exe
659902841 0x27555179 Zip archive data, at least v2.0 to extract, compressed
size: 24173, uncompressed size: 69081, name: NETCAT.C
659927076 0x2755B024 Zip archive data, at least v2.0 to extract, compressed
size: 28401, uncompressed size: 59392, name: nc.exe
659955517 0x27561F3D Zip archive data, at least v2.0 to extract, compressed
size: 3193, uncompressed size: 12039, name: doexec.c
659958748 0x27562BDC Zip archive data, at least v2.0 to extract, compressed
size: 288, uncompressed size: 544, name: makefile
659959074 0x27562D22 Zip archive data, at least v2.0 to extract, compressed
size: 7394, uncompressed size: 22784, name: getopt.c
659966506 0x27564A2A Zip archive data, at least v2.0 to extract, compressed
size: 3070, uncompressed size: 7283, name: generic.h
659969615 0x2756564F Zip archive data, at least v2.0 to extract, compressed
size: 24324, uncompressed size: 61780, name: hobbit.txt

Binwalk, Foremost, Strings & Bulk_Extractor Done And Displayed
Thank you

File Edit View Go Help

  kali  Desktop **hddDirectory**

Places

-  Computer
-  kali
-  Desktop
-  Trash
-  Documents
-  Music
-  Pictures
-  Videos
-  Downloads



foremost



Bulk



strings.txt



log.txt



binwalk.txt



hddfile

File Edit View Go Help



kali



Desktop

hddDirectory

foremost

Places



Computer



kali



Desktop



Trash



Documents



Music



Pictures



Videos



Downloads

Devices



gif



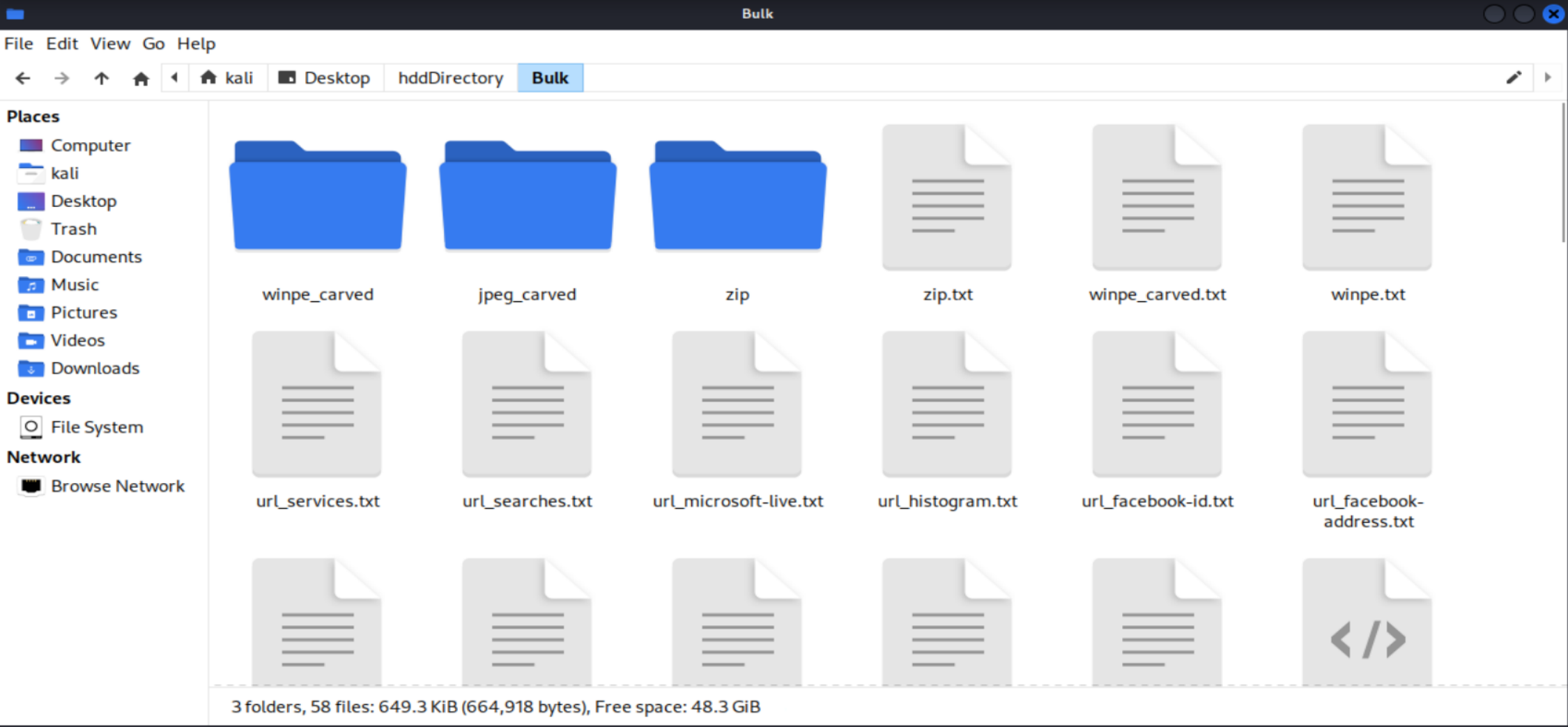
zip



log1.txt



audit.txt



Places

- Computer
- kali
- Desktop
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices

- File System

Network

- Browse Network

