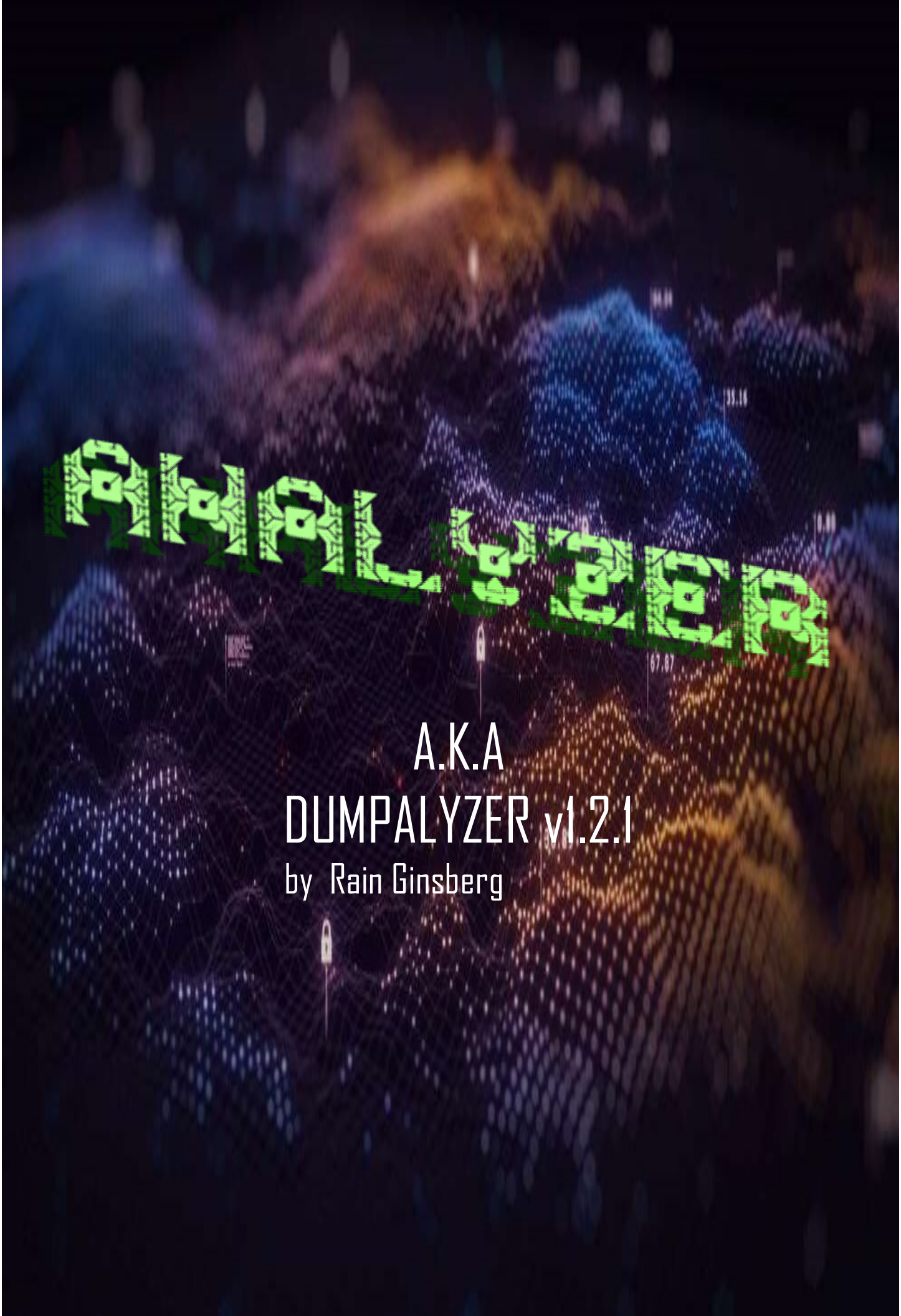
A.K.A
DUMPALYZER v1.2.1
by Rain Ginsberg

What is Analyzer?

Analyzer is a script made in bash, created to analyze Memory and HDD files, extracting them with several prolific forensic tools and organize their output in easy-to-find directories and log files.

```
Analyzer (AKA - Dumpalyzer v1.2.1)
Bakeneko, CrunchCorp LLC

    Correct usage: .\Analyzer.sh [mem \ hdd] [FILE]]
```

Analyzer syntax is composed of two user-defined variables. First is choosing between “MEM” or “HDD”, and the second is he name of the file in need of analyzing.

MEM file:

```
└─$ ./Analyzer.sh hdd carver.001
```

HDD file:

```
└─$ ./Analyzer.sh mem snowden.mem
```

Analyzer can run with bash command without giving it permissions with chmod.

```
└─$ bash Analyzer.sh hdd carver.001
```

The HDD option attached to the file will send the user into the HDD analyzing menu with its relevant programs.

```
Analyzer (AKA - Dumpalyzer v1.2.1)
Bakeneko, CrunchCorp LLC

[*] Analyzing HDD file - inv.ad1
[+] Directory created - inv.ad1-170822

HDD Analyzing options:
[1] Binwalk
[2] Strings
[3] Foremost
[4] Bulk Extractor
--------------------
[0] Exit Program

Choose:
```

HDD menu 3

The MEM option attached to the file will send the user into the Memory analyzing menu.

```
Analyzer (AKA - Dumpalyzer v1.2.1)
Bakeneko, CrunchCorp LLC

[*] Analyzing memory file - snowden.mem
[+] Directory created - snowden.mem-170822

MEM Analyzing Options:
[1] Volatility
[2] Strings
[3] Bulk Extractor
--------------------
[0] Exit Program

Choose:
```

Each program will ask the user for the help menu for the flags, so the user could choose from the list what to use with the program before it runs on the file.

Each time the user will choose not to see the help menu, the scrip will run a loop between 13 random sentences encrypted before-hand and decrypted to motivate the user for his knowledge of the program's flags.

```
Need to see the help menu for flags? (y/n): n

See, unlike most hackers, I get a little joy out of figuring out how to install the latest toy.
```

```
Need to see the help menu for flags? (y/n): n

Never underestimate the determination of a kid who is time-rice and cash-poor.
```

```
Need to see the help menu for flags? (y/n): n

There are few sources of energy so powerful as a procrastinating college student.
```

```
Need to see the help menu for flags? (y/n): n

They say that the Devil works hard.
```

The encrypted strings from the script:

```
array[0]="T2YgY291cnNlIG5vdCwgeW91IGtub3cgd2hhdCB5b3UgYXJlIGRvaW5nLg=="
array[1]="TmV2ZXIgdGVsbCBldmVyeXRoaW5nIHlvdSBrbm93Li4u"
array[2]="VGhlcmUgYXJlIG5vIHR3byB3b3JkcyBpbiB0aGUgZW5nbGlzaCBsYW5ndWFnZSBtb3JlIGhhcm1mdWwgdGhhbiAtIEdvb2QgSm9iLg=="
array[3]="U2VlLCB1bmxpa2UgbW9zdCBoYWNrZXJzLCBJIGdldCBhIGxpdHRsZSBqb3kgb3V0IG9mIGZpZ3VyaW5nIG91dCBob3cgdG8gaW5zdGFsbCB0aGUgbGF0ZXN0IHRveS4="
array[4]="QmVoaW5kIGV2ZXJ5IHN1Y2Nlc3NmdWwgQ29kZXIgdGhlcmUgYW4gZXZlbiBtb3JlIHN1Y2Nlc3NmdWwgRGUtY29kZXIgdG8gdW5kZXJzdGFuZCB0aGF0IGNvZGUu"
array[5]="VGhlcmUgYXJlIGZldyBzb3VyY2VzIG9mIGVuZXJneSBzbyBwb3dlcmZ1bCBhcyBhIHByb2NyYXN0aW5hdGluZyBjb2xsZWdlIHN0dWRlbnQu"
array[6]="TmV2ZXIgdW5kZXJlc3RpbWF0ZSB0aGUgZGV0ZXJtaW5hdGlvbiBvZiBhIGtpZCB3aG8gaXMgdGltZS1yaWNlIGFuZCBjYXNoLXBvb3Iu"
array[7]="RG9uJ3QgaGF0ZSBtZSwgaGF0ZSB0aGF0IGNvZGUu"
array[8]="VGltZSBpcyB3aGF0IGRldGVybWluZXMgc2VjdXJpdHkuIFdpdGggZW5vdWdoIHRpbWUgbm90aGluZyBpcyB1bmhhY2thYmxlLg=="
array[9]="RGFya25lc3MgZW52ZWxvcGVzIHRlY2hub2xvZ3kgd2hlcmUgb25seSBhIHNlbGVjdCBmZXcgZ2FpbiBhY2Nlc3MgdG8gdGhlIGxpZ2h0IHN3aXRjaC4="
array[10]="VGhleSBzYXkgdGhhdCB0aGUgRGV2aWwgd29ya3MgaGFyZC4="
array[11]="Tm90aGluZyB3aWxsIHdvcmsgdW5sZXNzIHlvdSBkby4="
array[12]="U3R1cGlkaXR5IGNvbWJpbmVkIHdpdGggYXJyb2dhbmNlIGFuZCBhIGh1Z2UgZWdvIHdpbGwgZ2V0IHlvdSBhIGxvbmcgd2F5Lg=="
```

Accepting the help menu of Binwalk will present these options:

```
Binwalk v2.3.3
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
    -Y, --disasm                Identify the CPU architecture of a file using the capstone disassembler
    -T, --minsn=<int>           Minimum number of consecutive instructions to be considered valid (default: 500)
    -k, --continue              Don't stop at the first match

Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence of bytes
    -A, --opcodes               Scan target file(s) for common executable opcode signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type[:ext[:cmd]]> Extract <type> signatures (regular expression), give the files an extension of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 levels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (default: current working directory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -0, --run-as=<str>          Execute external extraction utilities with the specified user's privileges
    -1, --preserve-symlinks     Do not sanitize extracted symlinks that point outside the extraction directory (dangerous)
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extraction utilities
    -V, --subdirs               Extract into sub-directories named by the offset

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analysis
    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold (default: 0.95)
--More--
```

Choosing a flag (or pressing “enter” for default extraction), the script will extract and present the directory named after binwalk and the current date.

```
Choose a flag for Binwalk (Press enter for default extraction):
-M
[+] Output directory created: binwalk-170822

HDD Analyzing options:
[1] Binwalk
[2] Strings
[3] Foremost
[4] Bulk Extractor
_____________________
[0] Exit Program

Choose:
```

“binwalk-170822” and in it an “output” directory of extracted files that Binwalk has carved.

```
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp/carver.001-170822]
└─$ ls -la
total 40
drwxr-xr-x  5 Bakeneko Bakeneko  4096 Aug 17 06:11 .
drwxr-xr-x 13 Bakeneko Bakeneko  4096 Aug 17 06:10 ..
drwxr-xr-x  3 Bakeneko Bakeneko  4096 Aug 17 06:10 binwalk-170822
drwxr-xr-x  3 Bakeneko Bakeneko  4096 Aug 17 06:11 bulk-ext-170822
drwxr-xr--  6 Bakeneko Bakeneko  4096 Aug 17 06:11 foremost-_Wed_Aug_17_06_11_25_2022
-rw-r--r--  1 Bakeneko Bakeneko 18648 Aug 17 06:11 strings-170822-1.txt
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp/carver.001-170822]
└─$ cd binwalk-170822
┌──(Bakeneko㉿kali)-[~/…/Scripts/temp/carver.001-170822/binwalk-170822]
└─$ ls -la
total 12
drwxr-xr-x 3 Bakeneko Bakeneko 4096 Aug 17 06:10 .
drwxr-xr-x 5 Bakeneko Bakeneko 4096 Aug 17 06:11 ..
drwxr-xr-x 2 Bakeneko Bakeneko 4096 Aug 17 06:10 output
```

Same with Strings:

```
Need to see the help menu for flags? (y/n): n

Never underestimate the determination of a kid who is time-rice and cash-poor.

Choose a flag for Strings (Press enter for default extraction):

[+] Strings: Extracting snowden.mem.
```

After extraction into log file, user is prompt with the question to view the log file in-program.

```
Would you like to view the extracted log file? (y/n) y
```

```
FACP_000_TABLEID = "FACP_000"
4550_TABLEID = "4550    "
HOFFA_TABLEID = "HOFFA    "
SERON_TABLEID = "SERONYXP"
K5_TABLEID = "K5      "
AWRDACPI_TABLEID = "AWRDACPI"
ND036_TABLEID = "ND000036"
BORG_TABLEID = "Borg    "
SERVIGIL_TABLEID = "SERVIGIL"
A003B_TABLEID = "A003B   "
CALISTGA_TABLEID = "CALISTGA"
NC6400_UMA_TABLEID = "30AD    "
NC6400_DISCRETE_TABLEID = "30AC    "
ALVISO_TABLEID = "ALVISO  "
DELLB8K_TABLEID = "B8K    "
A07_TABLEID = "A07     "
A08_TABLEID = "A08
 T40/T40p/T41/T41p/T42/T42p/R50/R50p/R51
                    {FACP.IBM_OEMID.TP-1S_TABLEID.*.*.*.*.0.0.0.0.0.0}, \ ; ThinkPad R40e
                    {FACP.IBM_OEMID.TP-1U_TABLEID.*.*.*.*.0.0.0.0.0.0}, \ ; ThinkPad X40
                    {FACP.IBM_OEMID.TP-1V_TABLEID.*.*.*.*.0.0.0.0.0.0}, \ ; ThinkPad R51
                    {FACP.IBM_OEMID.TP-1W_TABLEID.*.*.*.*.0.0.0.0.0.0}, \ ; ThinkPad R50e
```

```
fCfX
fSfRf
fIfKf
fKfI
fZf[
//home/Bakeneko/Documents/Scripts/temp/snowden.mem-160822/strings-160822-2.txt
```

```
[+] Output created: strings-170822-1.txt
```

Foremost:

```
Choose a flag for Foremost (Press enter for default extraction):
-a
[+] Foremost: Extracting inv.ad1. This may take some time.
```

```
Need to see the help menu for flags? (y/n): y
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
       [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
```

Foremost directory extracted:

```
└─$ cd foremost-_Wed_Aug_17_06_11_25_2022
┌──(Bakeneko㉿kali)-[~/…/Scripts/temp/carver.001-170822/foremost-_Wed_Aug_17_06_11_25_2022]
└─$ ls
audit.txt  docx  jpg  pdf  png
```

```
┌──(Bakeneko㉿kali)-[~/…/temp/carver.001-170822/foremost-_Wed_Aug_17_06_11_25_2022/jpg]
└─$ ls -la
total 80
drwxr-xr-- 2 Bakeneko Bakeneko  4096 Aug 17 06:11 .
drwxr-xr-- 6 Bakeneko Bakeneko  4096 Aug 17 06:11 ..
-rw-r--r-- 1 Bakeneko Bakeneko 70719 Aug 17 06:11 00000079.jpg
┌──(Bakeneko㉿kali)-[~/…/temp/carver.001-170822/foremost-_Wed_Aug_17_06_11_25_2022/jpg]
└─$ cd ..
┌──(Bakeneko㉿kali)-[~/…/Scripts/temp/carver.001-170822/foremost-_Wed_Aug_17_06_11_25_2022]
└─$ cd png
┌──(Bakeneko㉿kali)-[~/…/temp/carver.001-170822/foremost-_Wed_Aug_17_06_11_25_2022/png]
└─$ ls
00000232.png  00000252.png  00000298.png
```

Bulk Extractor help options:

```
ulk_extractor version 2.0.0: A high-performance flexible digital forensics program.
sage:
 bulk_extractor [OPTION...] image_name

 -A, --offset_add arg          Offset added (in bytes) to feature locations (default: 0)
 -b, --banner_file arg         Path of file whose contents are prepended to top of all feature files
 -C, --context_window arg      Size of context window reported in bytes (default: 16)
 -d, --debug arg               enable debugging (default: 1)
 -D, --debug_help              help on debugging
 -E, --enable_exclusive arg    disable all scanners except the one specified. Same as -x all -E scanner.
 -e, --enable arg              enable a scanner (can be repeated)
 -x, --disable arg             disable a scanner (can be repeated)
 -f, --find arg                search for a pattern (can be repeated)
 -F, --find_file arg           read patterns to search from a file (can be repeated)
 -G, --pagesize arg            page size in bytes (default: 16777216)
 -g, --marginsize arg          margin size in bytes (default: 4194304)
 -j, --threads arg             number of threads (default: 4)
 -J, --no_threads              read and process data in the primary thread
 -M, --max_depth arg           max recursion depth (default: 12)
     --max_bad_alloc_errors arg
                               max bad allocation errors (default: 3)
     --max_minute_wait arg     maximum number of minutes to wait until all data are read (default: 60)
     --notify_main_thread      Display notifications in the main thread after phase1 completes. Useful for running with ThreadSanitizer
     --notify_async            Display notificaitons asynchronously (default)
 -o, --outdir arg              output directory [REQUIRED]
 -P, --scanner_dir arg         directories for scanner shared libraries (can be repeated). Default directories include /usr/local/lib/bulk_extractor
                               /usr/lib/bulk_extractor and any directories specified in the BE_PATH environment variable.
 -p, --path arg                print the value of <path>[:length][/h][/r] with optional length, hex output, or raw output.
 -q, --quit                    no status or performance output
 -r, --alert_list arg          file to read alert list from
 -R, --recurse                 treat image file as a directory to recursively explore
 -S, --set arg                 set a name=value option (can be repeated)
 -s, --sampling arg            random sampling parameter frac[:passes]
 -V, --version                 Display PACKAGE_VERSION (currently) 2.0.0
 -w, --stop_list arg           file to read stop list from
 -Y, --scan arg                specify <start>[-end] of area on disk to scan
 -z, --page_start arg          specify a starting page number
 -Z, --zap                     wipe the output directory (recursively) before starting
 -0, --no_notify               disable real-time notification
 -1, --version1                version 1.0 notification (console-output)
 -H, --info_scanners           report information about each scanner
 -h, --help                    print help screen
```

```
[+] Bulk Extractor: Extracting snowden.mem. This may take some time.
[+] Output directory created: bulk-ext-170822
```

```
┌──(Bakeneko㉿kali)-[~/…/Scripts/temp/carver.001-170822/bulk-ext-170822]
└─$ ls -la
total 12
drwxr-xr-x 3 Bakeneko Bakeneko 4096 Aug 17 06:11 .
drwxr-xr-x 5 Bakeneko Bakeneko 4096 Aug 17 06:11 ..
drwxr-xr-x 3 Bakeneko Bakeneko 4096 Aug 17 06:11 output
┌──(Bakeneko㉿kali)-[~/…/Scripts/temp/carver.001-170822/bulk-ext-170822]
└─$ cd output
┌──(Bakeneko㉿kali)-[~/…/temp/carver.001-170822/bulk-ext-170822/output]
└─$ ls -s
total 108
 0 aes_keys.txt               4 email_histogram.txt     0 gps.txt                 0 ntfsusn_carved.txt    0 telephone_histogram.txt    0 utmp_carved.txt
 0 alerts.txt                 4 email.txt               0 httplogs.txt            0 pii_teamviewer.txt    0 telephone.txt              0 vcard.txt
 0 ccn_histogram.txt          0 ether_histogram_1.txt   0 ip_histogram.txt        0 pii.txt               0 unrar_carved.txt           0 windirs.txt
 0 ccn_track2_histogram.txt   0 ether_histogram.txt     0 ip.txt                  0 rar.txt               0 url_facebook-address.txt   0 winlnk.txt
 0 ccn_track2.txt             0 ether.txt               0 jpeg_carved.txt        12 report.xml            0 url_facebook-id.txt        0 winpe_carved.txt
 0 ccn.txt                    0 evtx_carved.txt         0 json.txt                0 rfc822.txt             4 url_histogram.txt          0 winpe.txt
 4 domain_histogram.txt       0 exif.txt                0 kml_carved.txt          0 sin.txt                0 url_microsoft-live.txt     0 winprefetch.txt
20 domain.txt                 0 facebook.txt            0 ntfsindx_carved.txt     0 sqlite_carved.txt      0 url_searches.txt           4 zip
 0 elf.txt                    0 find_histogram.txt      0 ntfslogfile_carved.txt  0 tcp_histogram.txt      4 url_services.txt          12 zip.txt
 4 email_domain_histogram.txt 0 find.txt                0 ntfsmft_carved.txt      0 tcp.txt               36 url.txt
┌──(Bakeneko㉿kali)-[~/…/temp/carver.001-170822/bulk-ext-170822/output]
└─$
```

Volatility needs a compatible profile to work, so when the program starts to run it will analyze the file for suggested profiles and will ask the user to choose one.

```
Analyzing memory file for compatible profiles required to use volatility.
 Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86

Choose a profile from the suggested list (Case-sensitive): VistaSP2x86

You have selected profile - VistaSP2x86.
Need to see the help menu for flags? (y/n):

Time is what determines security. With enough time nothing is unhackable.

Choose a flag for Volatility:
filescan

Would you like to view the extracted log file? (y/n)
```

Since Volatility cannot run without a flag, the program will get “stuck” in a while loop until user will chooses a flag. After a few times the script will suggest again the help menu.

```
Analyzing memory file for compatible profiles required to use volatility.
 Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86

Choose a profile from the suggested list (Case-sensitive): VistaSP2x86

You have selected profile - VistaSP2x86.
Choose a flag for Volatility:

You must choose a flag. Choose again:

Need to see the help menu for flags? (y/n):
You must choose a flag. Choose again:

Need to see the help menu for flags? (y/n):
You must choose a flag. Choose again:

Need to see the help menu for flags? (y/n):
You must choose a flag. Choose again:

Need to see the help menu for flags? (y/n): n

See, unlike most hackers, I get a little joy out of figuring out how to install the latest toy.

You must choose a flag. Choose again:

Need to see the help menu for flags? (y/n): n

They say that the Devil works hard.

You must choose a flag. Choose again: filescan
```

```
Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/Bakeneko/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/home/Bakeneko/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
                        the Module Output Options below)
  --output-file=OUTPUT_FILE
                        Write output in this file
  -v, --verbose         Verbose information
  -g KDBG, --kdbg=KDBG  Specify a KDBG virtual address (Note: for 64-bit
                        Windows 8 and above this is the address of
                        KdCopyDataBlock)
  --force               Force utilization of suspect profile
  -k KPCR, --kpcr=KPCR  Specify a specific KPCR address
  --cookie=COOKIE       Specify the address of nt!ObHeaderCookie (valid for
                        Windows 10 only)

        Supported Plugin Commands:

                amcache         Print AmCache information
                apihooks        Detect API hooks in process and kernel memory
--More--
```

```
Would you like to view the extracted log file? (y/n)
```

```
Offset(P)           #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x00000000001e4f10      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
0x00000000002e0260      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\resutils.dll
0x00000000002e06e8      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
0x00000000002e0980      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
0x000000000041b2c0      4      0 R--r-d \Device\HarddiskVolume1\Windows\System32\mscoree.dll
0x000000000041b458      5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\netfxperf.dll
0x000000000041b6d0      1      1 R--r-- \Device\HarddiskVolume1\Windows\Registration\R000000000018.clb
0x0000000000057ecc8      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
0x00000000005a5950      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6001.18000_none_9e752e5ac9c6
19f3
0x00000000005c9338      3      1 ------ \Device\NamedPipe\net\NtControlPipe20
0x00000000005c9ae0      2      1 ------ \Device\NamedPipe\lsass
0x0000000000650c38      3      1 ------ \Device\Afd\Endpoint
0x0000000000668298      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\wbem\wbemprox.dll
0x00000000006685d8      8      0 R--r-d \Device\HarddiskVolume1\Windows\System32\TPVMW32.dll
0x0000000000668a70      3      0 R--r-d \Device\HarddiskVolume1\Windows\System32\hnetcfg.dll
0x00000000006d1028      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
0x00000000006d1618      1      1 R--r-- \Device\HarddiskVolume1\Windows\Registration\R000000000018.clb
0x000000000078f028      8      0 R--r-d \Device\HarddiskVolume1\Windows\System32\wbem\cimwin32.dll
0x000000000078f6b8      5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\wbem\wmiprov.dll
0x00000000007eb2f0      1      1 ------ \Device\NamedPipe\net\NtControlPipe20
0x00000000007ebbc0      1      1 R--rw- \Device\HarddiskVolume1\Windows\System32
0x00000000007ef888      5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\framedynos.dll
0x00000000007efb90      3      1 ------ \Device\NamedPipe\net\NtControlPipe19
0x00000000007eff18      1      1 ------ \Device\NamedPipe\lsarpc
0x0000000000092e028      7      0 R--r-d \Device\HarddiskVolume1\Windows\System32\bthprops.cpl
0x0000000000092e128      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6001.18000_none_5cdb
aa5a083979cc
```

extracted directories. New files are not overwritten and followed by a sequential number.

```
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp]
└─$ cd snowden.mem-170822
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp/snowden.mem-170822]
└─$ ls
bulk-ext-170822  strings-170822-1.txt  vol-170822-1.txt  vol-170822-2.txt  vol-170822-3.txt
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp/snowden.mem-170822]
└─$ ls -la
total 15356
drwxr-xr-x  3 Bakeneko Bakeneko     4096 Aug 17 08:04 .
drwxr-xr-x 12 Bakeneko Bakeneko     4096 Aug 17 08:04 ..
drwxr-xr-x  2 Bakeneko Bakeneko     4096 Aug 17 06:09 bulk-ext-170822
-rw-r--r--  1 Bakeneko Bakeneko 15239975 Aug 17 06:07 strings-170822-1.txt
-rw-r--r--  1 Bakeneko Bakeneko   153314 Aug 17 05:55 vol-170822-1.txt
-rw-r--r--  1 Bakeneko Bakeneko   153314 Aug 17 06:07 vol-170822-2.txt
-rw-r--r--  1 Bakeneko Bakeneko   153314 Aug 17 08:03 vol-170822-3.txt
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp/snowden.mem-170822]
└─$
```

After each finished extraction, the MEM or HDD menu will be called again for the user to choose a different program for analyzing the file or to exit.

```
[+] Output created: vol-170822-2.txt

MEM Analyzing Options:
[1] Volatility
[2] Strings
[3] Bulk Extractor
------------------
[0] Exit Program

Choose:
```

Choosing 0 will end the script and exit the program.

```
Thank you for using Analyzer (AKA - Dumpalyzer v1.2.1)
Goodbye!
┌──(Bakeneko㉿kali)-[~/Documents/Scripts/temp]
└─$
```