V8

You will need to use the volatility plugin of pslist or pstree to list the processes and identify the parent nodejs process. Most of the times, the parent process will have the data within. There are applications which are powered with nodejs like electron. Electron can be also used to retrieve the objects from the memory.

Using pstree on

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/monero.vmem' --profile=Win10x64_18362 pstree
```

```
File  Edit  View  Search  Terminal  Help
... 0xffffc78cfe1dc0c0:chrome.exe                1036   4456      0 ------ 2021-10-04 03:02:01 UTC+0000
... 0xffffc78cfc1ef080:chrome.exe                6032   4456      0 ------ 2021-10-04 03:02:01 UTC+0000
... 0xffffc78d02a120c0:cmd.exe                   1988   3492      1      0 2022-03-19 05:48:28 UTC+0000
.... 0xffffc78cffdc9080:conhost.exe               276   1988      3      0 2022-03-19 05:48:28 UTC+0000
.... 0xffffc78d0478b080:node.exe                 8408   1988     13      0 2022-03-19 05:55:47 UTC+0000
..... 0xffffc78d03e9a080:cmd.exe                 5644   8408      1      0 2022-03-19 05:55:48 UTC+0000
..... 0xffffc78cfb75a4c0:node.exe                6512   5644      9      0 2022-03-19 05:55:48 UTC+0000
...... 0xffffc78d02c69080:cmd.exe                5740   6512      1      0 2022-03-19 05:55:48 UTC+0000
....... 0xffffc78cfea6e080:node.exe              7364   5740     13      0 2022-03-19 05:55:49 UTC+0000
........ 0xffffc78cfad95080:cmd.exe              6592   7364      1      0 2022-03-19 05:55:49 UTC+0000
......... 0xffffc78d01538080:node.exe            7588   6592      9      0 2022-03-19 05:55:49 UTC+0000
.......... 0xffffc78d04...80:node.exe           2128   7588     13      0 2022-03-19 05:55:50 UTC+0000
........... 0xffffc78d0...00:cmd.exe             6412   2128      1      0 2022-03-19 05:56:14 UTC+0000
............ 0xffffc78c...80:node.exe          2864   6412     13      0 2022-03-19 05:56:15 UTC+0000
............. 0xffffc78...00:cmd.exe            8500   2864      1      0 2022-03-19 05:56:15 UTC+0000
.............. 0xffffc7...80:node.exe            272   8500      9      0 2022-03-19 05:56:15 UTC+0000
............... 0xffffc...80:cmd.exe             6356    272      1      0 2022-03-19 05:56:15 UTC+0000
................ 0xffff...80:node.exe           4928   6356      9      0 2022-03-19 05:56:15 UTC+0000
................. 0xfff...80:electron.exe       5016   4928     32      0 2022-03-19 05:56:16 UTC+0000
.................. 0xff...80:electron.exe       1228   5016     18      0 2022-03-19 05:56:22 UTC+0000
................... 0xf...c0:xmr-stak.exe        1048   1228     10      0 2022-03-19 06:14:37 UTC+0000
.................... 0x...c0:conhost.exe         4436   1048      2      0 2022-03-19 06:14:37 UTC+0000
................... 0xff...80:electron.exe       6932   5016      7      0 2022-03-19 05:56:19 UTC+0000
... 0xffffc78cfe7eb080:chrome.exe                5452   3492     28      0 2022-03-19 05:45:46 UTC+0000
```

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/nodejs.agario.ver14.15.1.vmem' --profile=Win10x64_18362 ps
tree
```

```
.... 0xffffbf014e755080:node.exe                 1644   5096     11      0 2020-11-29 10:12:41 UTC+0000
.... 0xffffbf014f696080:conhost.exe              3060   5096      5      0 2020-11-29 10:11:12 UTC+0000
. 0xffffbf014d4a5340:fontdrvhost.ex               824    556      5      0 2020-11-29 10:03:28 UTC+0000
. 0xffffbf014d585340:dwm.exe                      984    556     15      0 2020-11-29 10:03:30 UTC+0000
 0xffffbf014ccdf280:csrss.exe                     492    484     12      0 2020-11-29 10:03:24 UTC+0000
```

Task 3

We use v8_findalltypes to find the all the types of objects. Some of the have unknown name we can still extract them. The plugin will list the name of known in the first column, on the second column it will list the instance address type then the count in the memory in the third column.

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/monero.vmem' --profile=Win10x64_18362 v8_findalltypes
Volatility Foundation Volatility Framework 2.6.1
Enter PID: 5016
Scanning electron.exe pid: 5016
Meta Map Address: 0x3cdb6982258
New Meta Map Value : 0x3cdb6982259
Name
                          Instance Type Map Count

                                 17139        37

                                   186       315

                                   191         3
Invalid Typename
                                   755         2

                                   193         1
Invalid Typename
```

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/nodejs.agario.ver14.15.1.vmem' --profile=Win10x64_18362 v8
_findalltypes
```

```
Uint32Array                     1051        1
Int32Array                      1051        1
[Symbol.toPrimitive]            1041        1
Float64Array                    1051        1
ReferenceError                  1069        1
Int8Array                       1051        1
Invalid Typename                1041        1
has                             1054        1
EvalError                       1069        1
Uint16Array                     1051        1
ArrayBuffer                     1061        2
Uint8Array                      1051        1
finally                         1076        1
Number                          1041        1
Int16Array                      1051        1
test                            1077        3
Function                        1091        9
Boolean                         1041        1
String                          1041        1
Float32Array                    1051        1
TypeError                       1069        1
Array                           1060       11
BigUint64Array                  1051        1
ERR_INVALID_THIS                1057        1
```

The next plugin is v8_instancetypeaddr to find the objects using the instance type.

For example from the above we can see that there's 315 maps for 186 instancetype or 1041.

That's why we used in the plugin specifically when we were prompted to enter *instance number*.

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/monero.vmem' --profile=Win10x64_18362 v8_instancetypeaddr
Volatility Foundation Volatility Framework 2.6.1
Enter PID: 5016
Scanning electron.exe pid: 5016
Meta Map Address: 0x3cdb6982258
New Meta Map Value : 0x3cdb6982259
Please enter the Instance Number: 186
Instance Number entered: 186
Enter Max number of objects: 1
Number    Object Address    Instance Type    Data
1         0x15eb71032a0L         0xba         {}
2         0x2b5798f0078L         0xba         {None: 4364230468433}
```

```
v8@ubuntu: ~/volatility
File  Edit  View  Search  Terminal  Help
byM                             1057        8
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/nodejs.agario.ver14.15.1.vmem' --profile=Win10x64_18362 v8
_instancetypeaddr
Volatility Foundation Volatility Framework 2.6.1
Enter PID: 1644
Scanning node.exe pid: 1644
Meta Map Address: 0x1ae17f80168
New Meta Map Value : 0x1ae17f80169
Please enter the Instance Number: 1041
Instance Number entered: 1041
Enter Max number of objects: 1
Number    Object Address    Instance Type    Data
1         0x1a916f66700L         0x411        {}
2         0x344bd6006e8L         0x411        {}
3         0x344bd616108L         0x411        {'trim': 3593769933137, '': 3593769936721, 'toLocaleUpperCase': 3593769936553, 'trimStart': 3593769919953, 'valueOf': 35
93769917945, 'blink': 3593769925161, 'matchAll': 3593769915057, 'substr': 3593769925753, 'charCodeAt': 3593769913105, 'charAt': 3593769935601, 'normalize': 35937699
35937, 'startsWith': 3593769936441, 'slice': 3593769930321, 'sub': 3593769936329, 'length': 1436675474929, 'padEnd': 3593769934505, 'toString': 3593769936497, 'spli
t': 3593769906897, 'localeCompare': 3593769935881, 'sup': 3593769936385, 'strike': 3593769936273, 'fontcolor': 3593769935713, 'match': 3593769934353, 'repeat': 3593
769936049, 'lastIndexOf': 3593769931377, 'bold': 3593769934201, 'indexOf': 3593769935825, 'big': 3593769935545, 'trimRight': 3593769925905, 'includes': 359376992483
3, 'fontsize': 3593769905849, 'replace': 3593769936105, 'toLocaleLowerCase': 3593769916321, 'concat': 3593769901337, 'substring': 3593769932985, 'search': 359376993
6161, 'italics': 3593769931033, 'toLowerCase': 3593769936609, 'trimLeft': 3593769919953, 'padStart': 3593769935993, 'toUpperCase': 3593769936665, 'endsWith': 359376
9935657, 'constructor': 3593769934737, 'small': 3593769936217, 'link': 3593769913985, 'fixed': 3593769935769, 'trimEnd': 3593769925905, 'anchor': 3593769909313, 'co
dePointAt': 3593769902161}
v8@ubuntu:~/volatility$
```

Extract properties plugin

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/monero.vmem' --profile=Win10x64_18362 v8_extractprops
Volatility Foundation Volatility Framework 2.6.1
Enter PID: 5016
Enter Instance Type Hex: 0x8
Scanning electron.exe pid: 5016
Meta Map Address: 0x3cdb6982258
New Meta Map Value : 0x3cdb6982259
Enter Max number of objects: 100
```

```
v8@ubuntu:~/volatility$ python vol.py --plugins='/home/v8/volatility/contrib/plugins/' -f '/home/v8/dumps/nodejs.agario.ver14.15.1.vmem' --profile=Win10x64_18362 v8
_extractprops
Volatility Foundation Volatility Framework 2.6.1
Enter PID: 1644
Enter Instance Type Hex: 0x8
Scanning node.exe pid: 1644
Meta Map Address: 0x1ae17f80168
New Meta Map Value : 0x1ae17f80169
Enter Max number of objects: 300
```

A file will be created in the same path where the bash is currently operating on. For example,

```
v8@ubuntu:~/volatility$ pwd
/home/v8/volatility
```

The file will be at */home/v8/volatility/extractProperties.txt*

You can *hexedit* or *hexviewer* to view the content of the file.

```
v8@ubuntu:~/volatility$ hexedit extractProperties.txt
```

```
v8@ubuntu: ~/volatility
File  Edit  View  Search  Terminal  Help
00000000   0A 66 6F 72  6B 0A 52 6F  75 6E 64 52  6F 62 69 6E  48 61 6E 64  6C 65 0A 53  68 61 72 65  64 48 61 6E  64 6C 65 0A  .fork.RoundRobinHandle.SharedHandle.
00000024   57 6F 72 6B  65 72 0A 73  65 6E 64 48  65 6C 70 65  72 0A 69 6E  74 65 72 63  6F 6D 0A 53  43 48 45 44  5F 4E 4F 4E  Worker.sendHelper.intercom.SCHED_NON
00000048   45 0A 53 43  48 45 44 5F  52 52 0A 6D  69 6E 50 6F  72 74 0A 6D  61 78 50 6F  72 74 0A 64  65 62 75 67  50 6F 72 74  E.SCHED_RR.minPort.maxPort.debugPort
0000006C   4F 66 66 73  65 74 0A 69  6E 69 74 69  61 6C 69 7A  65 64 0A 73  63 68 65 64  75 6C 69 6E  67 50 6F 6C  69 63 79 0A  Offset.initialized.schedulingPolicy.
00000090   73 65 74 75  70 53 65 74  74 69 6E 67  73 4E 54 0A  63 72 65 61  74 65 57 6F  72 6B 65 72  50 72 6F 63  65 73 73 0A  setupSettingsNT.createWorkerProcess.
000000B4   72 65 6D 6F  76 65 57 6F  72 6B 65 72  0A 72 65 6D  6F 76 65 48  61 6E 64 6C  65 73 46 6F  72 57 6F 72  6B 65 72 0A  removeWorker.removeHandlesForWorker.
000000D8   65 6D 69 74  46 6F 72 6B  4E 54 0A 6F  6E 6C 69 6E  65 0A 65 78  69 74 65 64  41 66 74 65  72 44 69 73  63 6F 6E 6E  emitForkNT.online.exitedAfterDisconn
000000FC   65 63 74 0A  71 75 65 72  79 53 65 72  76 65 72 0A  69 6E 74 65  72 6E 61 6C  2F 63 6C 75  73 74 65 72  2F 72 6F 75  ect.queryServer.internal/cluster/rou
00000120   6E 64 5F 72  6F 62 69 6E  5F 68 61 6E  64 6C 65 0A  69 6E 74 65  72 6E 61 6C  2F 63 6C 75  73 74 65 72  2F 73 68 61  nd_robin_handle.internal/cluster/sha
00000144   72 65 64 5F  68 61 6E 64  6C 65 0A 69  6E 74 65 72  6E 61 6C 2F  63 6C 75 73  74 65 72 2F  77 6F 72 6B  65 72 0A 69  red_handle.internal/cluster/worker.i
00000168   6E 74 65 72  6E 61 6C 2F  63 6C 75 73  74 65 72 2F  75 74 69 6C  73 0A 69 73  57 6F 72 6B  65 72 0A 77  6F 72 6B 65  nternal/cluster/utils.isWorker.worke
0000018C   72 73 0A 4E  4F 44 45 5F  43 4C 55 53  54 45 52 5F  53 43 48 45  44 5F 50 4F  4C 49 43 59  0A 72 72 0A  73 65 74 75  rs.NODE_CLUSTER_SCHED_POLICY.rr.setu
000001B0   70 4D 61 73  74 65 72 0A  67 65 74 56  61 6C 69 64  53 74 64 69  6F 0A 73 65  74 75 70 43  68 61 6E 6E  65 6C 0A 43  pMaster.getValidStdio.setupChannel.C
000001D4   68 69 6C 64  50 72 6F 63  65 73 73 0A  73 74 64 69  6F 53 74 72  69 6E 67 54  6F 41 72 72  61 79 0A 4D  41 58 5F 42  hildProcess.stdioStringToArray.MAX_B
000001F8   55 46 46 45  52 0A 6E 6F  72 6D 61 6C  69 7A 65 45  78 65 63 41  72 67 73 0A  6E 6F 72 6D  61 6C 69 7A  65 53 70 61  UFFER.normalizeExecArgs.normalizeSpa
0000021C   77 6E 41 72  67 75 6D 65  6E 74 73 0A  73 70 61 77  6E 0A 73 70  61 77 6E 53  79 6E 63 0A  63 68 65 63  6B 45 78 65  wnArguments.spawn.spawnSync.checkExe
00000240   63 53 79 6E  63 45 72 72  6F 72 0A 76  61 6C 69 64  61 74 65 54  69 6D 65 6F  75 74 0A 76  61 6C 69 64  61 74 65 4D  cSyncError.validateTimeout.validateM
00000264   61 78 42 75  66 66 65 72  0A 73 61 6E  69 74 69 7A  65 4B 69 6C  6C 53 69 67  6E 61 6C 0A  63 75 73 74  6F 6D 50 72  axBuffer.sanitizeKillSignal.customPr
00000288   6F 6D 69 73  65 45 78 65  63 46 75 6E  63 74 69 6F  6E 0A 65 78  65 63 46 69  6C 65 0A 65  78 65 63 46  69 6C 65 53  omiseExecFunction.execFile.execFileS
000002AC   79 6E 63 0A  65 78 65 63  53 79 6E 63  0A 64 67 72  61 6D 0A 50  72 6F 63 65  73 73 0A 55  44 50 0A 6B  53 74 61 74  ync.execSync.dgram.Process.UDP.kStat
000002D0   65 53 79 6D  62 6F 6C 0A  53 6F 63 6B  65 74 4C 69  73 74 53 65  6E 64 0A 53  6F 63 6B 65  74 4C 69 73  74 52 65 63  eSymbol.SocketListSend.SocketListRec
000002F4   65 69 76 65  0A 4D 41 58  5F 48 41 4E  44 4C 45 5F  52 45 54 52  41 4E 53 4D  49 53 53 49  4F 4E 53 0A  6B 49 73 55  eive.MAX_HANDLE_RETRANSMISSIONS.kIsU
00000318   73 65 64 41  73 53 74 64  69 6F 0A 68  61 6E 64 6C  65 43 6F 6E  76 65 72 73  69 6F 6E 0A  66 6C 75 73  68 53 74 64  sedAsStdio.handleConversion.flushStd
---  extractProperties.txt       --0x0/0x1809----------
```

The more max objects. The more strings you can view.