Forensic Engine

udurrani.com

I am working on a tool that would gather some useful information and do forensics on different OS's like Windows, MAC and Linux / Unix. The idea is to start with a command line version that could be easily used by any one. Folks with some scripting knowledge can automate the command line and run things more efficiently. First I thought I would add everything to the same engine but then i changed my mind and split the project into multiple binaries, that way things could be used outside the frame work as well. Eventually I will wrap this with a GUI.

Some of the things this frame work can do:

- System Information
- File information
- File search
- Hash search
- Interface with well known engines like VirusTotal, FireEye and WildFire (As long as you have the key)
- Signature check: User can make any signatures or multiple signatures and apply to a file
- Binary check
- Binary header info
- File Header info
- Basic packet capture
- Processes using IP's and ports
- Create memory dumps (32 bit support at the moment)
- Get process list and get process children
- Snap shots: E.g. registry or folder snap shot for later comparisons.
- Drivers and services

And many more. In this write up I am going to include few use cases. All use cases were tested against windows 2012 R2 and windows 7. Comments are welcome. Please email me at

admin@udurrani.com

VIDEO LINK (With few use cases): https://youtu.be/l88-m8IM-OQ

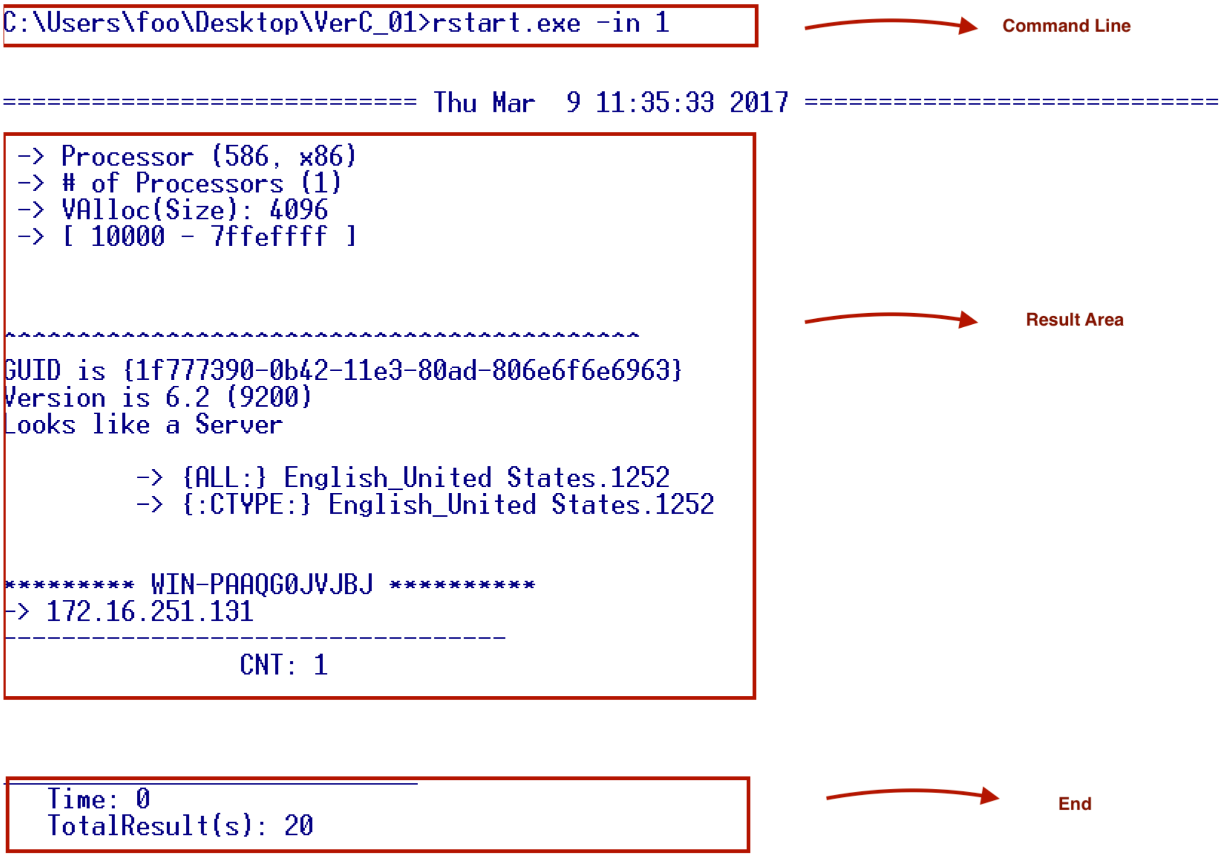
VIDEO LINK (Use case for malware activity feature MAF)

https://www.youtube.com/watch?v=-GrHtds2QQs

FrameWork has a very straight forward approach.

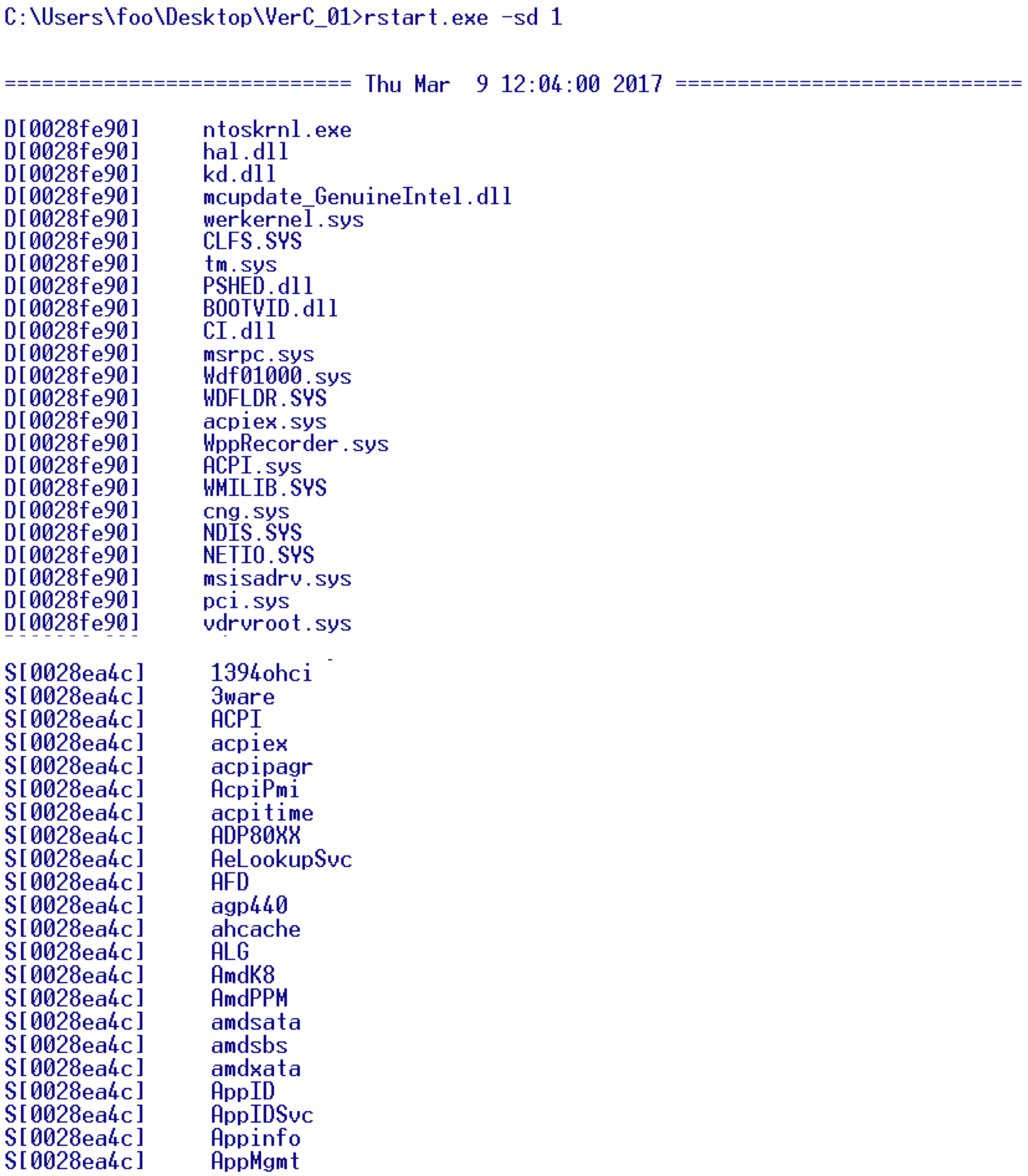
- *Command Line*
- *Result*
- *Footer*

In the following **use case** I am trying to get basic info about the computer:



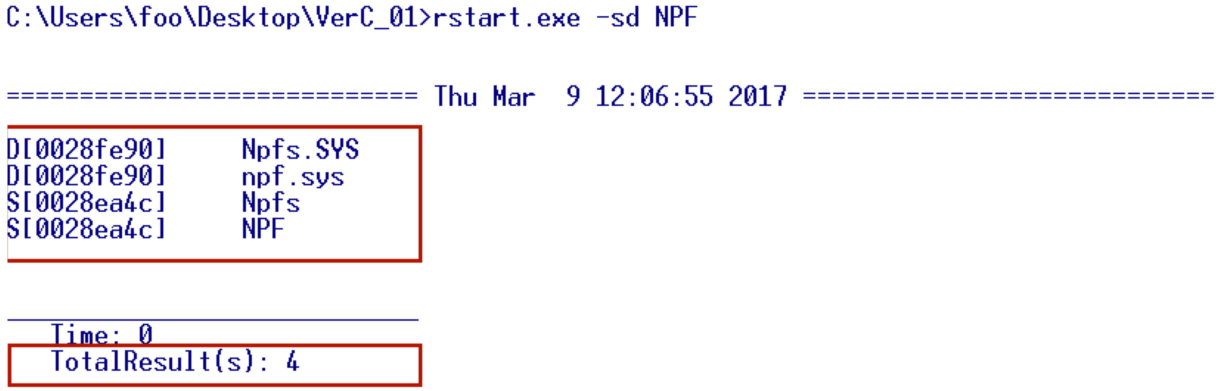
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -in 1

============================ Thu Mar  9 11:35:33 2017 ============================
 -> Processor (586, x86)
 -> # of Processors (1)
 -> VAlloc(Size): 4096
 -> [ 10000 - 7ffeffff ]



^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

GUID is {1f777390-0b42-11e3-80ad-806e6f6e6963}
Version is 6.2 (9200)
Looks like a Server

         -> {ALL:} English_United States.1252
         -> {:CTYPE:} English_United States.1252


********* WIN-PAAQG0JVJBJ **********
-> 172.16.251.131
----------------------------------
               CNT: 1


  Time: 0
  TotalResult(s): 20
```

In the following **use case** I am trying to gather all drivers and services running



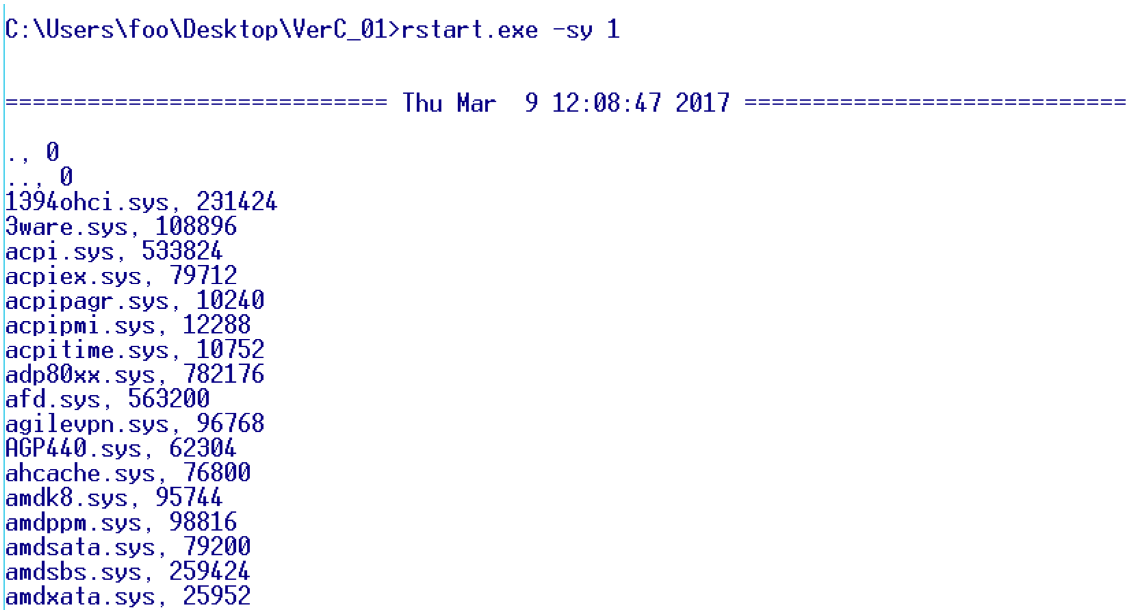
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -sd 1

============================ Thu Mar  9 12:04:00 2017 ============================

D[0028fe90]     ntoskrnl.exe
D[0028fe90]     hal.dll
D[0028fe90]     kd.dll
D[0028fe90]     mcupdate_GenuineIntel.dll
D[0028fe90]     werkernel.sys
D[0028fe90]     CLFS.SYS
D[0028fe90]     tm.sys
D[0028fe90]     PSHED.dll
D[0028fe90]     BOOTVID.dll
D[0028fe90]     CI.dll
D[0028fe90]     msrpc.sys
D[0028fe90]     Wdf01000.sys
D[0028fe90]     WDFLDR.SYS
D[0028fe90]     acpiex.sys
D[0028fe90]     WppRecorder.sys
D[0028fe90]     ACPI.sys
D[0028fe90]     WMILIB.SYS
D[0028fe90]     cng.sys
D[0028fe90]     NDIS.SYS
D[0028fe90]     NETIO.SYS
D[0028fe90]     msisadrv.sys
D[0028fe90]     pci.sys
D[0028fe90]     vdrvroot.sys

S[0028ea4c]      1394ohci
S[0028ea4c]      3ware
S[0028ea4c]      ACPI
S[0028ea4c]      acpiex
S[0028ea4c]      acpipagr
S[0028ea4c]      AcpiPmi
S[0028ea4c]      acpitime
S[0028ea4c]      ADP80XX
S[0028ea4c]      AeLookupSvc
S[0028ea4c]      AFD
S[0028ea4c]      agp440
S[0028ea4c]      ahcache
S[0028ea4c]      ALG
S[0028ea4c]      AmdK8
S[0028ea4c]      AmdPPM
S[0028ea4c]      amdsata
S[0028ea4c]      amdsbs
S[0028ea4c]      amdxata
S[0028ea4c]      AppID
S[0028ea4c]      AppIDSvc
S[0028ea4c]      Appinfo
S[0028ea4c]      AppMgmt
```

If you noticed I am ending the command line with ‘1’. If I use any other string, it will try to search for it E.g.



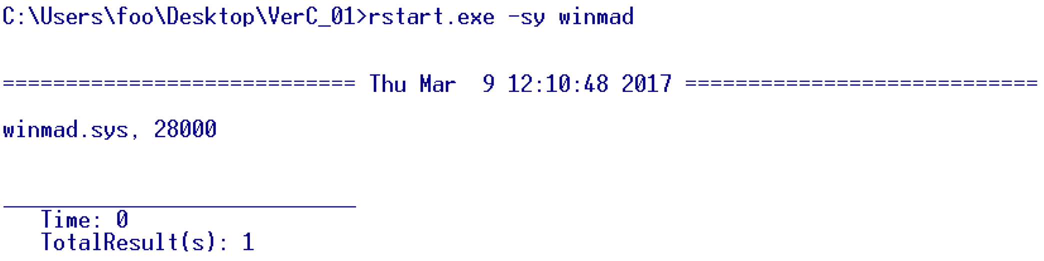
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -sd NPF

============================ Thu Mar  9 12:06:55 2017 ============================
D[0028fe90]      Npfs.SYS
D[0028fe90]      npf.sys
S[0028ea4c]      Npfs
S[0028ea4c]      NPF

____________________________
   Time: 0
   TotalResult(s): 4
```

Use case to find all sys files, their size. This can also be done in a snap shot manner



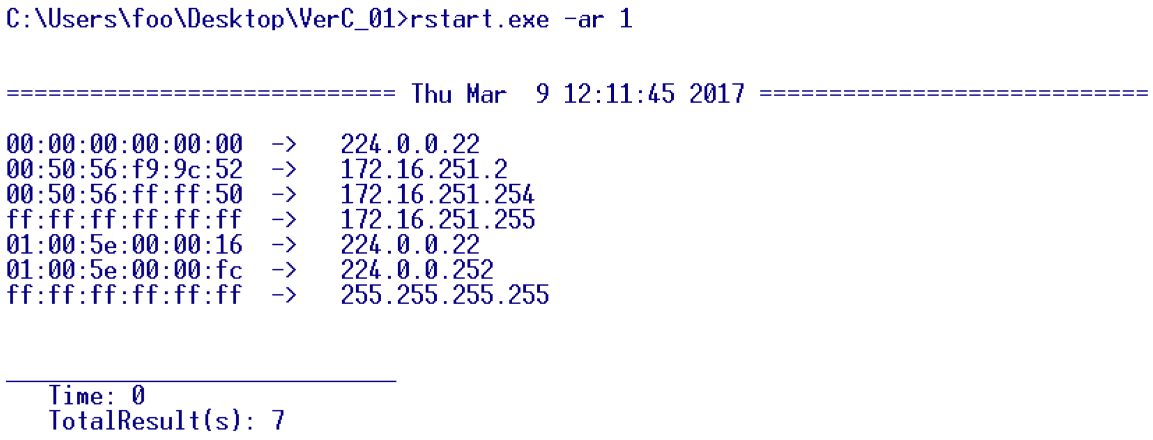
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -sy 1

============================ Thu Mar  9 12:08:47 2017 ============================

., 0
.., 0
1394ohci.sys, 231424
3ware.sys, 108896
acpi.sys, 533824
acpiex.sys, 79712
acpipagr.sys, 10240
acpipmi.sys, 12288
acpitime.sys, 10752
adp80xx.sys, 782176
afd.sys, 563200
agilevpn.sys, 96768
AGP440.sys, 62304
ahcache.sys, 76800
amdk8.sys, 95744
amdppm.sys, 98816
amdsata.sys, 79200
amdsbs.sys, 259424
amdxata.sys, 25952
```

Similarly for searching:

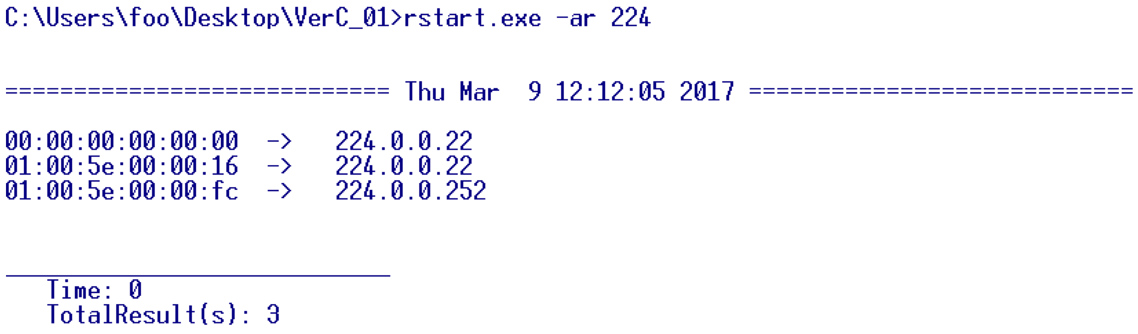


```
C:\Users\foo\Desktop\VerC_01>rstart.exe -sy winmad

============================ Thu Mar  9 12:10:48 2017 ============================

winmad.sys, 28000


____________________________
   Time: 0
   TotalResult(s): 1
```

Use case to get ARP information:

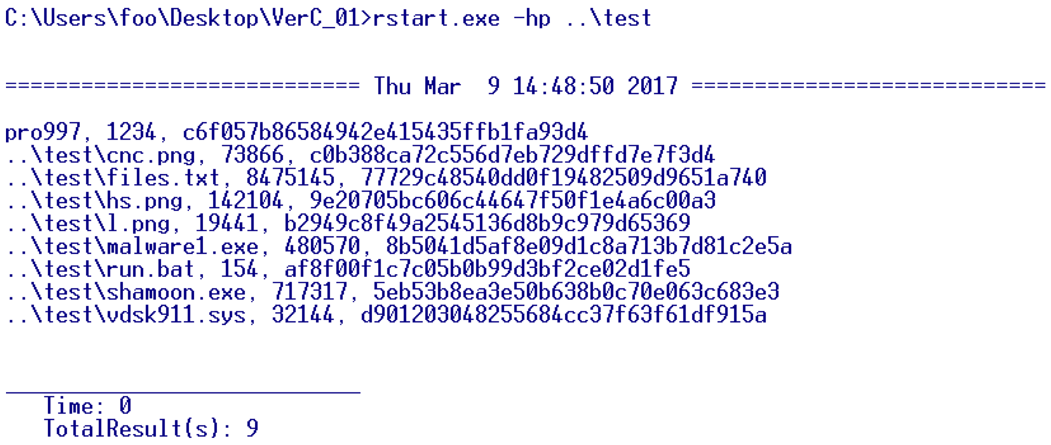


```
C:\Users\foo\Desktop\VerC_01>rstart.exe -ar 1


============================ Thu Mar  9 12:11:45 2017 ============================

00:00:00:00:00:00  ->   224.0.0.22
00:50:56:f9:9c:52  ->   172.16.251.2
00:50:56:ff:ff:50  ->   172.16.251.254
ff:ff:ff:ff:ff:ff  ->   172.16.251.255
01:00:5e:00:00:16  ->   224.0.0.22
01:00:5e:00:00:fc  ->   224.0.0.252
ff:ff:ff:ff:ff:ff  ->   255.255.255.255


____________________________
   Time: 0
   TotalResult(s): 7
```



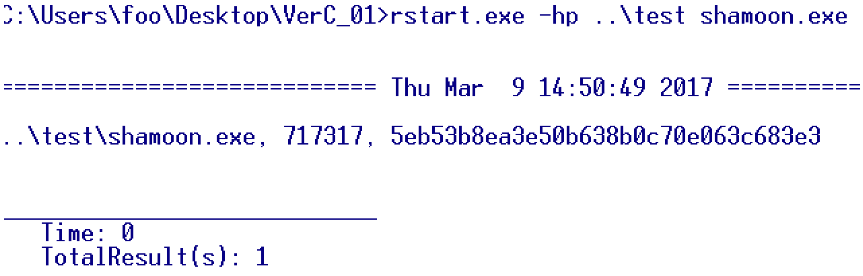
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -ar 224


============================ Thu Mar  9 12:12:05 2017 ============================

00:00:00:00:00:00  ->   224.0.0.22
01:00:5e:00:00:16  ->   224.0.0.22
01:00:5e:00:00:fc  ->   224.0.0.252


____________________________
   Time: 0
   TotalResult(s): 3
```

Use case to search for hashes, their size and names with a specific path



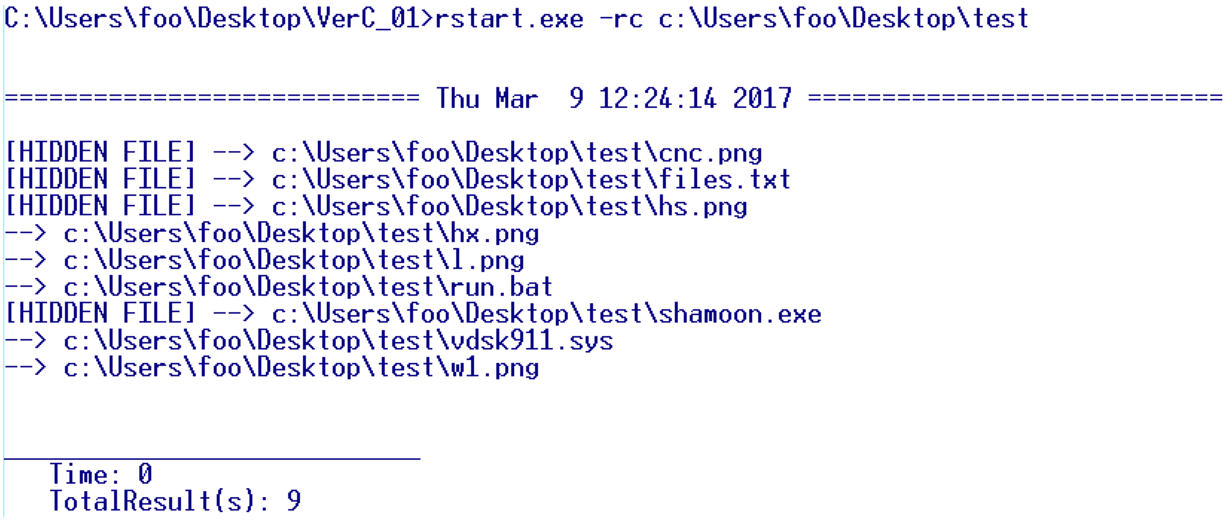
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -hp ..\test


========================== Thu Mar  9 14:48:50 2017 ==========================

pro997, 1234, c6f057b86584942e415435ffb1fa93d4
..\test\cnc.png, 73866, c0b388ca72c556d7eb729dffd7e7f3d4
..\test\files.txt, 8475145, 77729c48540dd0f19482509d9651a740
..\test\hs.png, 142104, 9e20705bc606c44647f50f1e4a6c00a3
..\test\l.png, 19441, b2949c8f49a2545136d8b9c979d65369
..\test\malware1.exe, 480570, 8b5041d5af8e09d1c8a713b7d81c2e5a
..\test\run.bat, 154, af8f00f1c7c05b0b99d3bf2ce02d1fe5
..\test\shamoon.exe, 717317, 5eb53b8ea3e50b638b0c70e063c683e3
..\test\vdsk911.sys, 32144, d901203048255684cc37f63f61df915a


___________________________
   Time: 0
   TotalResult(s): 9
```

Similarly for searching specific name



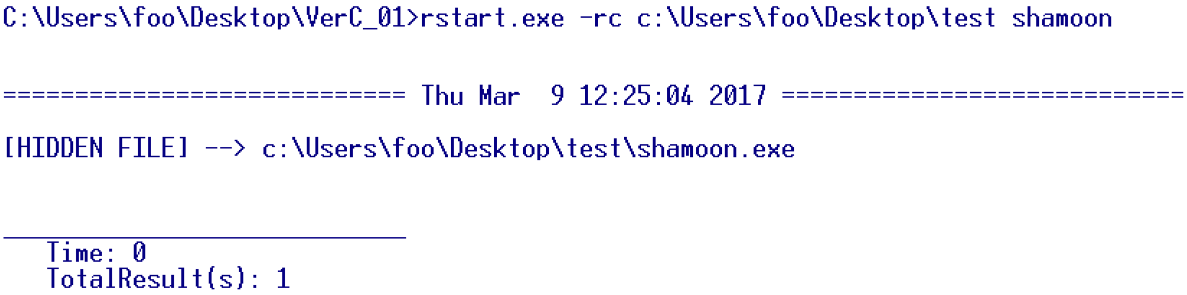
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -hp ..\test shamoon.exe

=========================== Thu Mar  9 14:50:49 2017 ============================

..\test\shamoon.exe, 717317, 5eb53b8ea3e50b638b0c70e063c683e3


___________________________
   Time: 0
   TotalResult(s): 1
```

Use case to look for hidden files in any folder. This search is recursive in nature



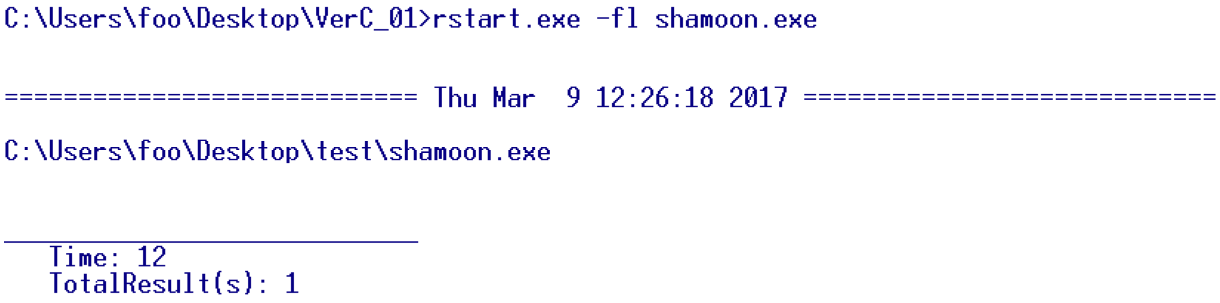
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -rc c:\Users\foo\Desktop\test


============================ Thu Mar  9 12:24:14 2017 ============================

[HIDDEN FILE] --> c:\Users\foo\Desktop\test\cnc.png
[HIDDEN FILE] --> c:\Users\foo\Desktop\test\files.txt
[HIDDEN FILE] --> c:\Users\foo\Desktop\test\hs.png
--> c:\Users\foo\Desktop\test\hx.png
--> c:\Users\foo\Desktop\test\l.png
--> c:\Users\foo\Desktop\test\run.bat
[HIDDEN FILE] --> c:\Users\foo\Desktop\test\shamoon.exe
--> c:\Users\foo\Desktop\test\vdsk911.sys
--> c:\Users\foo\Desktop\test\w1.png


____________________________
   Time: 0
   TotalResult(s): 9
```

For search:



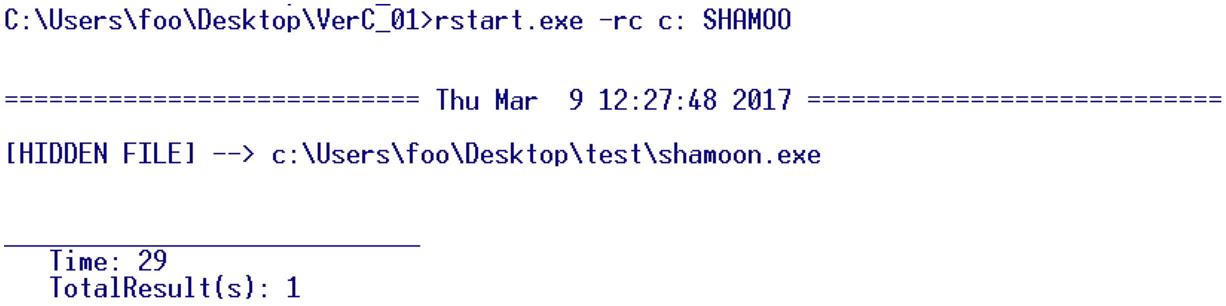
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -rc c:\Users\foo\Desktop\test shamoon

=========================== Thu Mar  9 12:25:04 2017 ============================

[HIDDEN FILE] --> c:\Users\foo\Desktop\test\shamoon.exe


___________________________
   Time: 0
   TotalResult(s): 1
```

Use case to search for a file without any path (ExactName MUST be used)



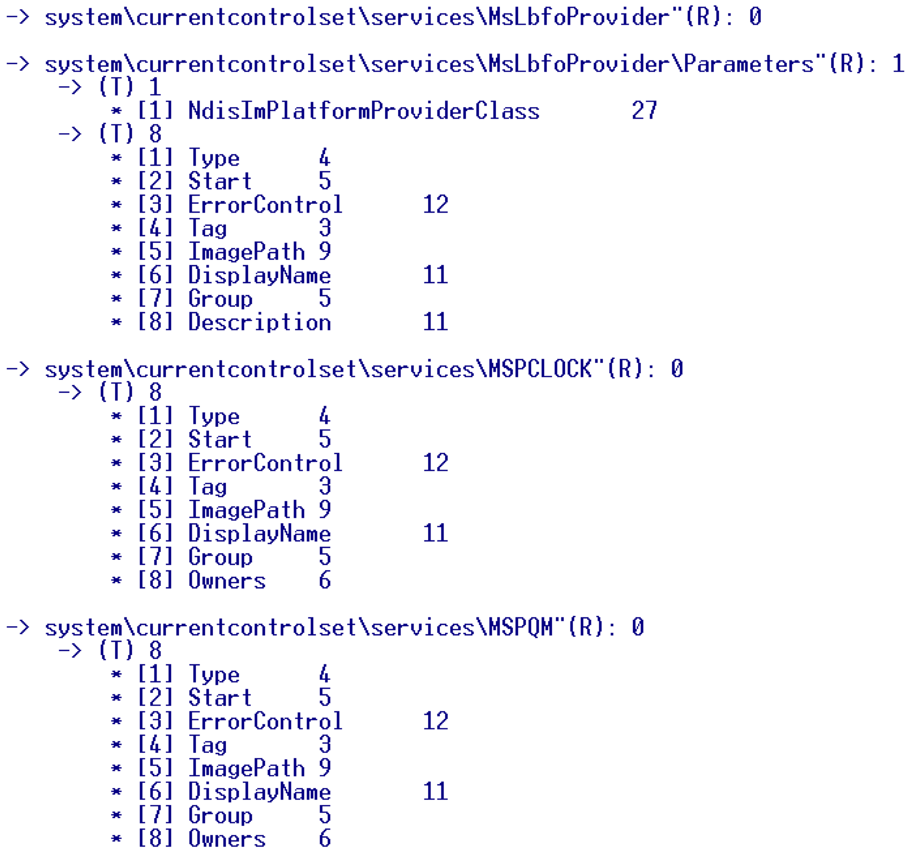
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -fl shamoon.exe

============================ Thu Mar  9 12:26:18 2017 ============================

C:\Users\foo\Desktop\test\shamoon.exe


____________________________
   Time: 12
   TotalResult(s): 1
```

Similar **use case** but a little slower with attribution (ExactName **not** required)



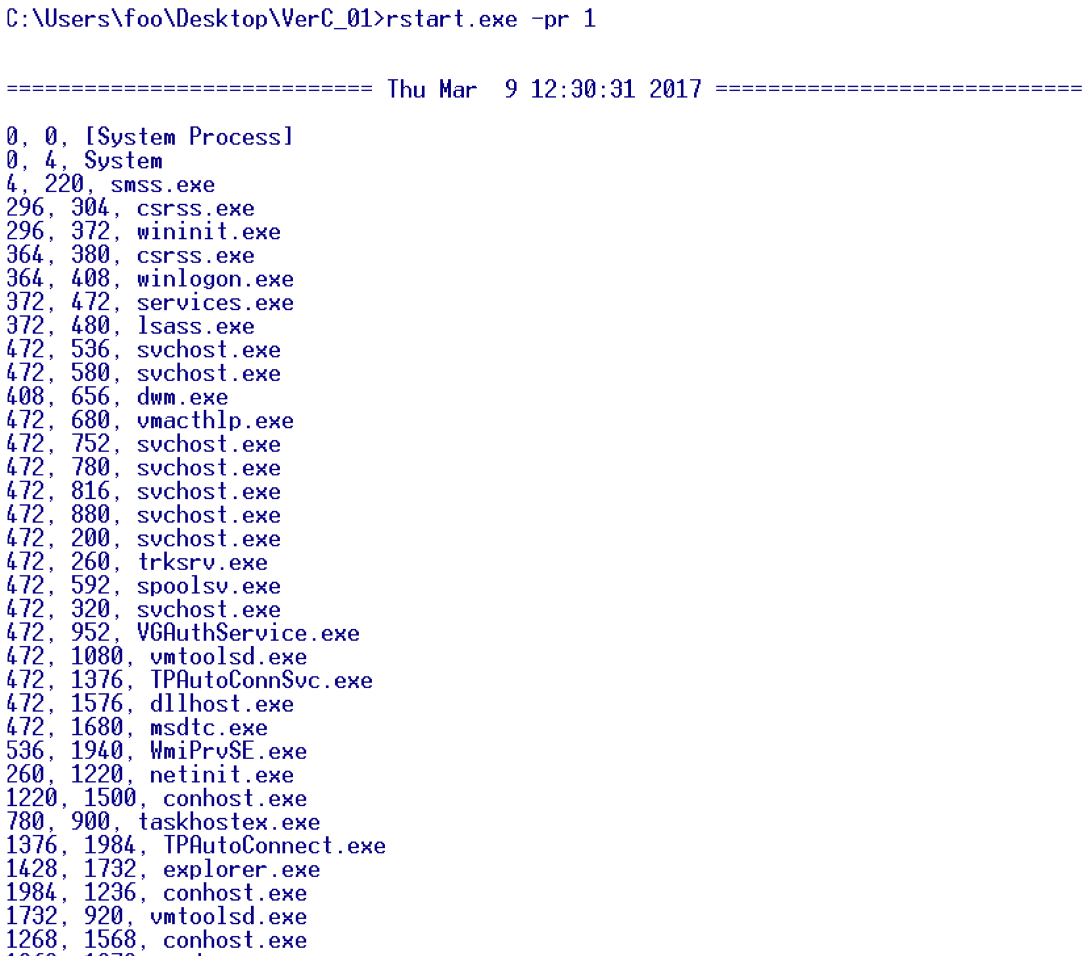
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -rc c: SHAMOO

============================ Thu Mar  9 12:27:48 2017 ============================

[HIDDEN FILE] --> c:\Users\foo\Desktop\test\shamoon.exe


____________________________
   Time: 29
   TotalResult(s): 1
```

Use case to search the registry and its depth



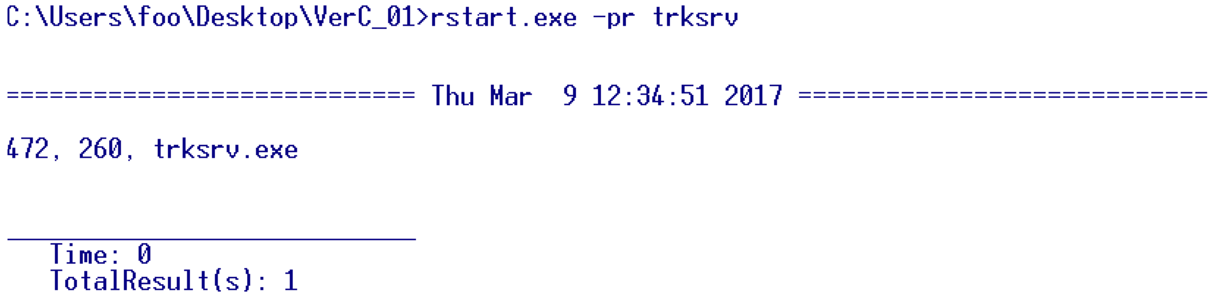
```
   -> system\currentcontrolset\services\MsLbfoProvider"(R): 0

   -> system\currentcontrolset\services\MsLbfoProvider\Parameters"(R): 1
       -> (T) 1
           * [1] NdisImPlatformProviderClass       27
       -> (T) 8
           * [1] Type      4
           * [2] Start     5
           * [3] ErrorControl      12
           * [4] Tag       3
           * [5] ImagePath 9
           * [6] DisplayName       11
           * [7] Group     5
           * [8] Description       11

   -> system\currentcontrolset\services\MSPCLOCK"(R): 0
       -> (T) 8
           * [1] Type      4
           * [2] Start     5
           * [3] ErrorControl      12
           * [4] Tag       3
           * [5] ImagePath 9
           * [6] DisplayName       11
           * [7] Group     5
           * [8] Owners    6

   -> system\currentcontrolset\services\MSPQM"(R): 0
       -> (T) 8
           * [1] Type      4
           * [2] Start     5
           * [3] ErrorControl      12
           * [4] Tag       3
           * [5] ImagePath 9
           * [6] DisplayName       11
           * [7] Group     5
           * [8] Owners    6
```

Use case to search for all processes, PPID, PID, Name. user can easily take a snap shot



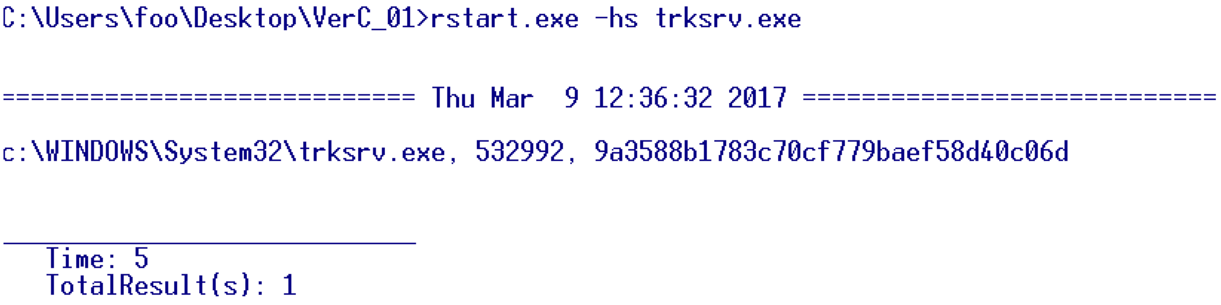
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -pr 1

============================ Thu Mar  9 12:30:31 2017 ============================

0, 0, [System Process]
0, 4, System
4, 220, smss.exe
296, 304, csrss.exe
296, 372, wininit.exe
364, 380, csrss.exe
364, 408, winlogon.exe
372, 472, services.exe
372, 480, lsass.exe
472, 536, svchost.exe
472, 580, svchost.exe
408, 656, dwm.exe
472, 680, vmacthlp.exe
472, 752, svchost.exe
472, 780, svchost.exe
472, 816, svchost.exe
472, 880, svchost.exe
472, 200, svchost.exe
472, 260, trksrv.exe
472, 592, spoolsv.exe
472, 320, svchost.exe
472, 952, VGAuthService.exe
472, 1080, vmtoolsd.exe
472, 1376, TPAutoConnSvc.exe
472, 1576, dllhost.exe
472, 1680, msdtc.exe
536, 1940, WmiPrvSE.exe
260, 1220, netinit.exe
1220, 1500, conhost.exe
780, 900, taskhostex.exe
1376, 1984, TPAutoConnect.exe
1428, 1732, explorer.exe
1984, 1236, conhost.exe
1732, 920, vmtoolsd.exe
1268, 1568, conhost.exe
```

Search ONLY for one of the famous shamoon process



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -pr trksrv

============================ Thu Mar  9 12:34:51 2017 ============================

472, 260, trksrv.exe


________________________________
   Time: 0
   TotalResult(s): 1
```

<span style="color:red">**Use case**</span> to look for the hash and size of this shamoon process binary



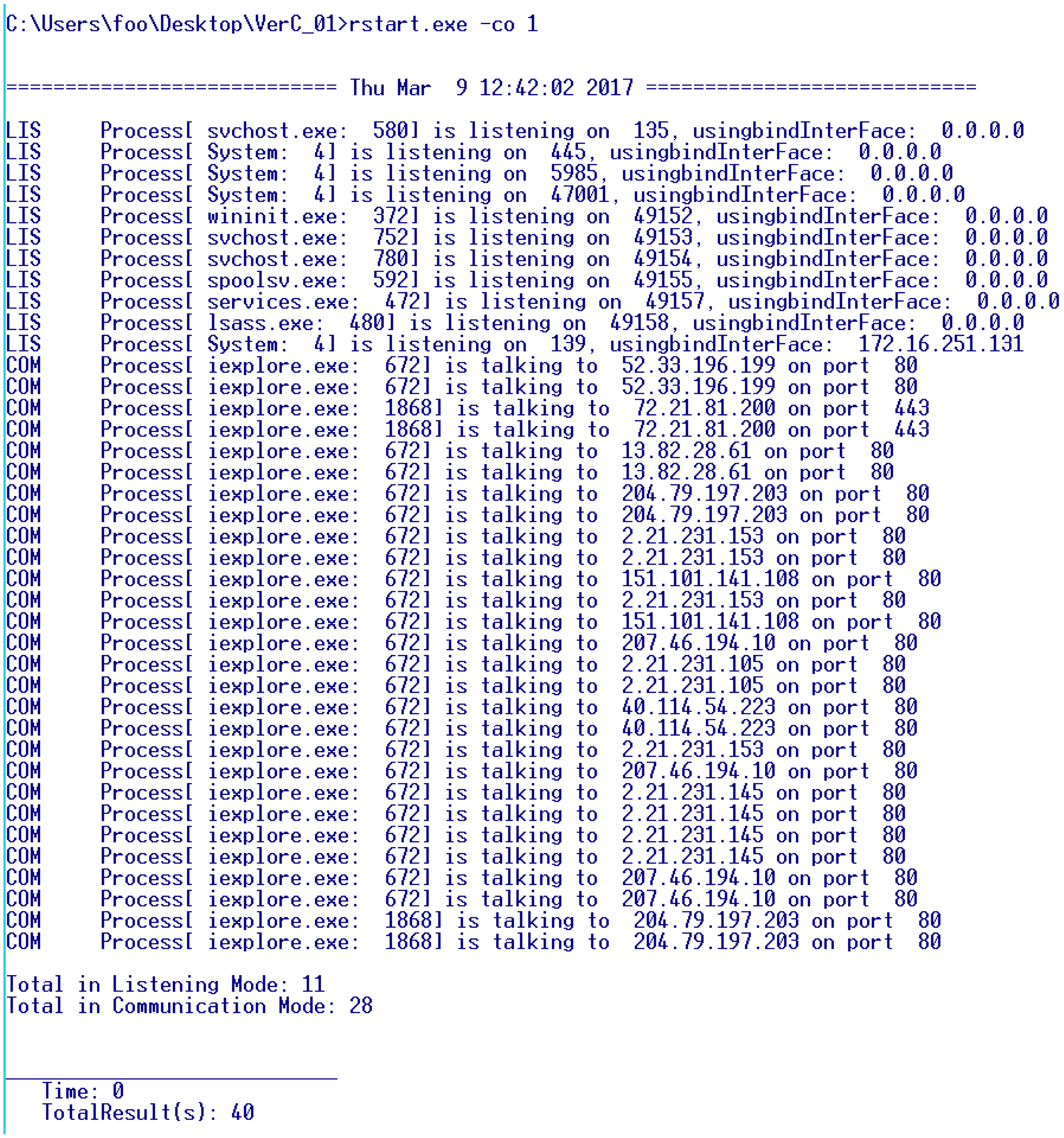
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -hs trksrv.exe

============================ Thu Mar  9 12:36:32 2017 ============================

c:\WINDOWS\System32\trksrv.exe, 532992, 9a3588b1783c70cf779baef58d40c06d


____________________________
   Time: 5
   TotalResult(s): 1
```

Use case to look for all the connections i.e. processes in listen state or processes that are communicating outbound.

LIS = LISTEN

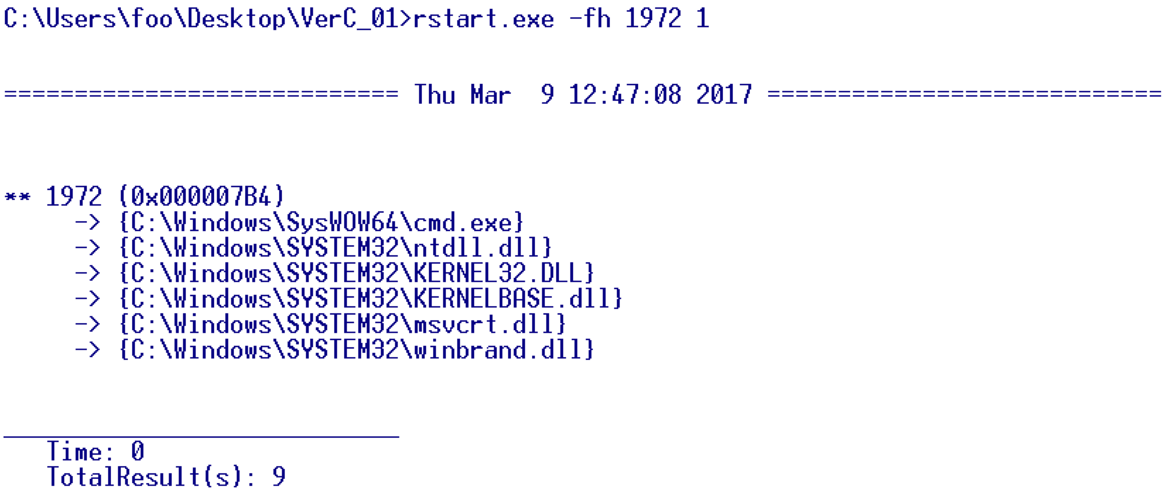
COM = Communicating

Process [Processname: PID]



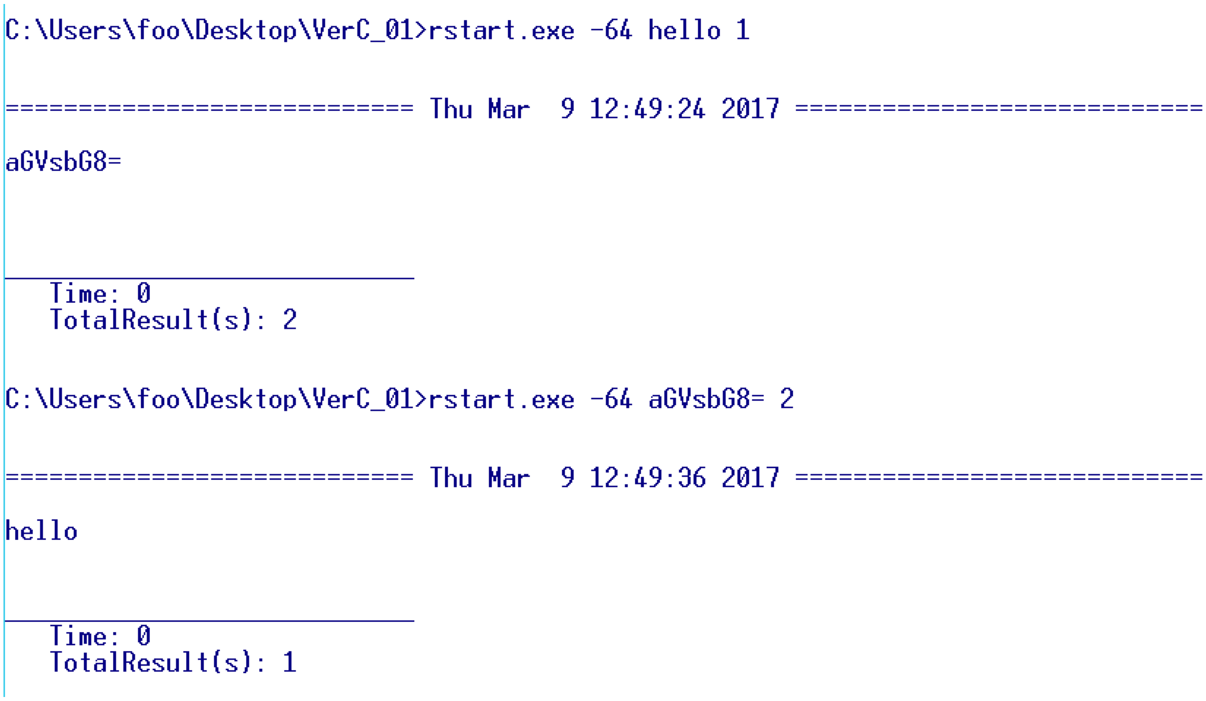
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -co 1

============================ Thu Mar  9 12:42:02 2017 ============================

LIS     Process[ svchost.exe:  580] is listening on  135, usingbindInterFace:  0.0.0.0
LIS     Process[ System:  4] is listening on  445, usingbindInterFace:  0.0.0.0
LIS     Process[ System:  4] is listening on  5985, usingbindInterFace:  0.0.0.0
LIS     Process[ System:  4] is listening on  47001, usingbindInterFace:  0.0.0.0
LIS     Process[ wininit.exe:  372] is listening on  49152, usingbindInterFace:  0.0.0.0
LIS     Process[ svchost.exe:  752] is listening on  49153, usingbindInterFace:  0.0.0.0
LIS     Process[ svchost.exe:  780] is listening on  49154, usingbindInterFace:  0.0.0.0
LIS     Process[ spoolsv.exe:  592] is listening on  49155, usingbindInterFace:  0.0.0.0
LIS     Process[ services.exe:  472] is listening on  49157, usingbindInterFace:  0.0.0.0
LIS     Process[ lsass.exe:  480] is listening on  49158, usingbindInterFace:  0.0.0.0
LIS     Process[ System:  4] is listening on  139, usingbindInterFace:  172.16.251.131
COM     Process[ iexplore.exe:  672] is talking to  52.33.196.199 on port  80
COM     Process[ iexplore.exe:  672] is talking to  52.33.196.199 on port  80
COM     Process[ iexplore.exe:  1868] is talking to  72.21.81.200 on port  443
COM     Process[ iexplore.exe:  1868] is talking to  72.21.81.200 on port  443
COM     Process[ iexplore.exe:  672] is talking to  13.82.28.61 on port  80
COM     Process[ iexplore.exe:  672] is talking to  13.82.28.61 on port  80
COM     Process[ iexplore.exe:  672] is talking to  204.79.197.203 on port  80
COM     Process[ iexplore.exe:  672] is talking to  204.79.197.203 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.153 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.153 on port  80
COM     Process[ iexplore.exe:  672] is talking to  151.101.141.108 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.153 on port  80
COM     Process[ iexplore.exe:  672] is talking to  151.101.141.108 on port  80
COM     Process[ iexplore.exe:  672] is talking to  207.46.194.10 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.105 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.105 on port  80
COM     Process[ iexplore.exe:  672] is talking to  40.114.54.223 on port  80
COM     Process[ iexplore.exe:  672] is talking to  40.114.54.223 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.153 on port  80
COM     Process[ iexplore.exe:  672] is talking to  207.46.194.10 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.145 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.145 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.145 on port  80
COM     Process[ iexplore.exe:  672] is talking to  2.21.231.145 on port  80
COM     Process[ iexplore.exe:  672] is talking to  207.46.194.10 on port  80
COM     Process[ iexplore.exe:  672] is talking to  207.46.194.10 on port  80
COM     Process[ iexplore.exe:  1868] is talking to  204.79.197.203 on port  80
COM     Process[ iexplore.exe:  1868] is talking to  204.79.197.203 on port  80

Total in Listening Mode: 11
Total in Communication Mode: 28


____________________________
   Time: 0
   TotalResult(s): 40
```

Use case to get handles of a process or DLL's



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -fh 1972 1

============================ Thu Mar  9 12:47:08 2017 ============================


** 1972 (0x000007B4)
     -> {C:\Windows\SysWOW64\cmd.exe}
     -> {C:\Windows\SYSTEM32\ntdll.dll}
     -> {C:\Windows\SYSTEM32\KERNEL32.DLL}
     -> {C:\Windows\SYSTEM32\KERNELBASE.dll}
     -> {C:\Windows\SYSTEM32\msvcrt.dll}
     -> {C:\Windows\SYSTEM32\winbrand.dll}


____________________________
   Time: 0
   TotalResult(s): 9
```

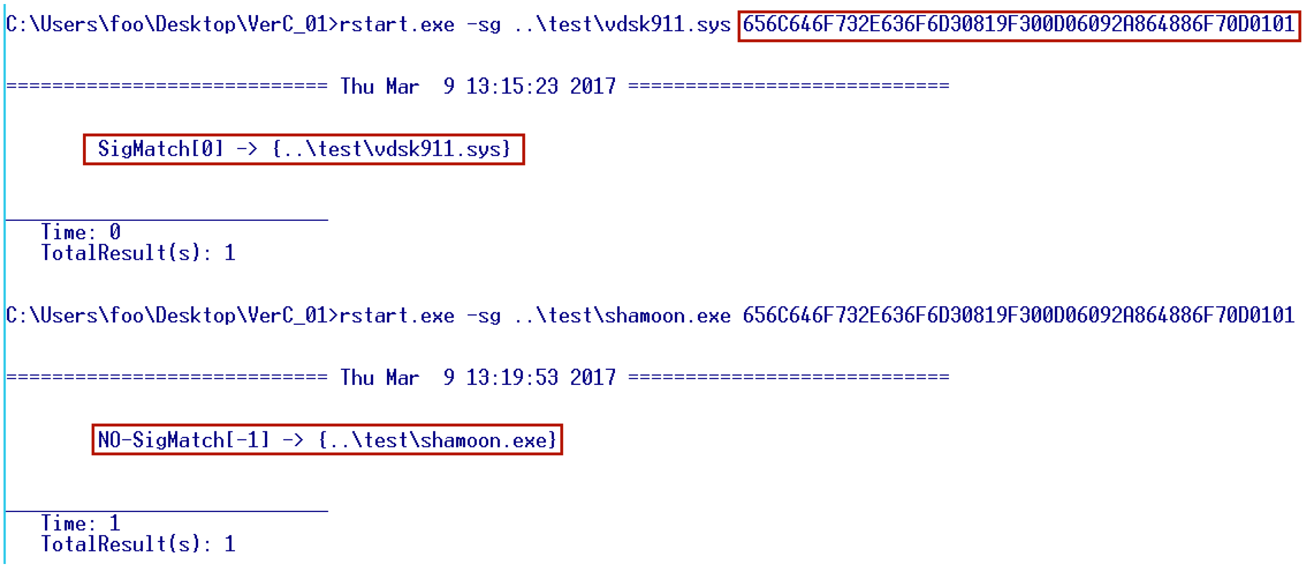
Use case to convert into to from base64



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -64 hello 1

============================ Thu Mar  9 12:49:24 2017 ============================

aGVsbG8=



____________________________
   Time: 0
   TotalResult(s): 2

C:\Users\foo\Desktop\VerC_01>rstart.exe -64 aGVsbG8= 2

============================ Thu Mar  9 12:49:36 2017 ============================

hello


____________________________
   Time: 0
   TotalResult(s): 1
```

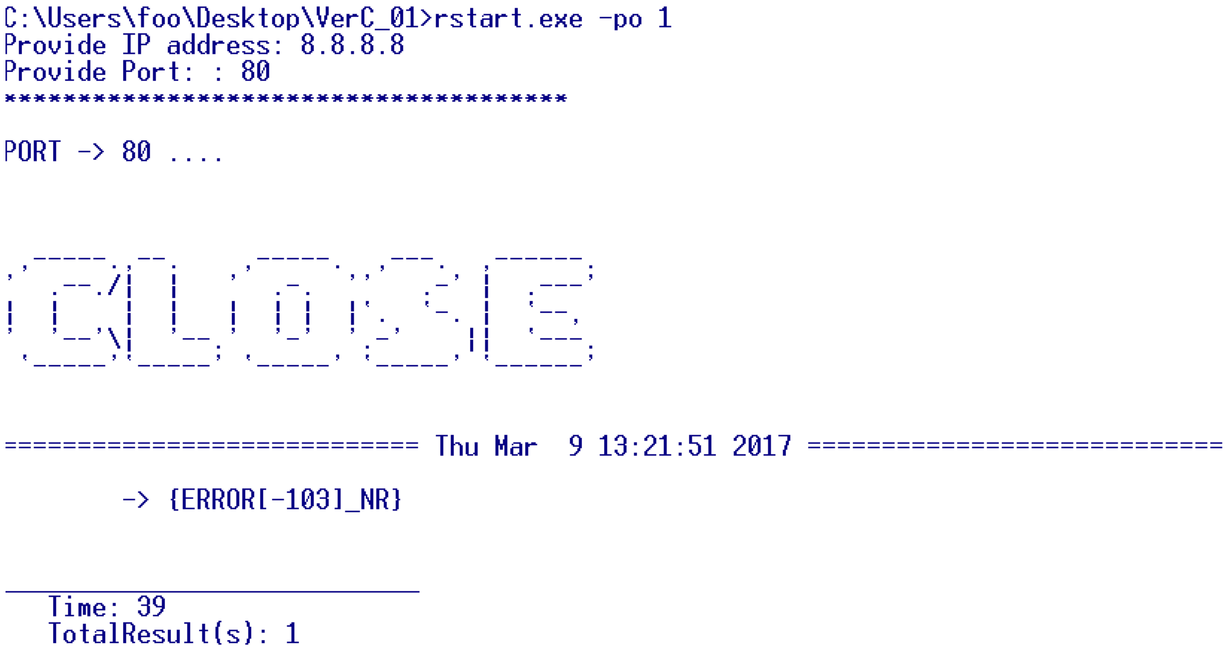
Use case to check for signatures. User can make signature(s) for this process and easily apply to any file. Process could be automated very easily as well with recursive process. Very simple example: SigMatch[0] = SUCCESS and signature match.

NOTE: Signature is not a file HASH



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -sg ..\test\vdsk911.sys 656C646F732E636F6D30819F300D06092A864886F70D0101

=========================== Thu Mar  9 13:15:23 2017 ===========================


       SigMatch[0] -> {..\test\vdsk911.sys}


___________________________
   Time: 0
   TotalResult(s): 1

C:\Users\foo\Desktop\VerC_01>rstart.exe -sg ..\test\shamoon.exe 656C646F732E636F6D30819F300D06092A864886F70D0101

=========================== Thu Mar  9 13:19:53 2017 ===========================


       NO-SigMatch[-1] -> {..\test\shamoon.exe}


___________________________
   Time: 1
   TotalResult(s): 1
```

Use case to scan a port on local or remote machine

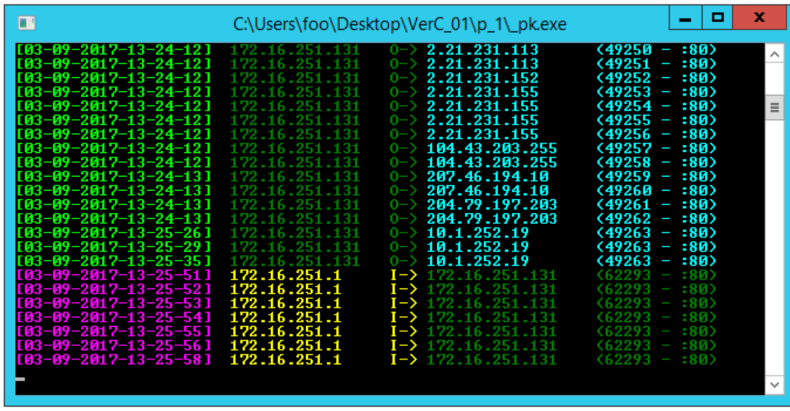


```
C:\Users\foo\Desktop\VerC_01>rstart.exe -po 1
Provide IP address: 8.8.8.8
Provide Port: : 80
****************************************

PORT -> 80 ....



 ,_____.,__.    ,_____.  ,___.  ,______;
,  .__./|  |   ,  ._.  ,,   :_, |  .___'
|  |    |  |   |  | |  |'.  '_. |  '__,
,  ,__,\|  ,__;,  ,_,  ,:_,    ||  '___
 '_____,'_____; '_____, '_____, '______;


=========================== Thu Mar  9 13:21:51 2017 ===========================

         -> {ERROR[-103]_NR}


___________________________
   Time: 39
   TotalResult(s): 1
```

Use case to capture TCP traffic in real-time. The effort here is to profile the end-point or a server. Not to capture the payloads. This will show who the end-point / server is really communicating to. The command line opens a new window and it keeps running.

O = Outgoing
I = Incoming

```
C:\Users\foo\Desktop\VerC_01>rstart.exe -pk 1

============================ Thu Mar  9 13:22:51 2017 ============================

        -> {ERROR[-103]_NR}

____________________________
   Time: 0
   TotalResult(s): 1

C:\Users\foo\Desktop\VerC_01>
```



C:\Users\foo\Desktop\VerC_01\p_1_pk.exe

```
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.113     <49250 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.113     <49251 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.152     <49252 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.155     <49253 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.155     <49254 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.155     <49255 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 2.21.231.155     <49256 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 104.43.203.255   <49257 - :80>
[03-09-2017-13-24-12]  172.16.251.131   O-> 104.43.203.255   <49258 - :80>
[03-09-2017-13-24-13]  172.16.251.131   O-> 207.46.194.10    <49259 - :80>
[03-09-2017-13-24-13]  172.16.251.131   O-> 207.46.194.10    <49260 - :80>
[03-09-2017-13-24-13]  172.16.251.131   O-> 204.79.197.203   <49261 - :80>
[03-09-2017-13-24-13]  172.16.251.131   O-> 204.79.197.203   <49262 - :80>
[03-09-2017-13-25-26]  172.16.251.131   O-> 10.1.252.19      <49263 - :80>
[03-09-2017-13-25-29]  172.16.251.131   O-> 10.1.252.19      <49263 - :80>
[03-09-2017-13-25-35]  172.16.251.131   O-> 10.1.252.19      <49263 - :80>
[03-09-2017-13-25-51]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-52]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-53]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-54]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-55]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-56]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
[03-09-2017-13-25-58]  172.16.251.1     I-> 172.16.251.131   <62293 - :80>
_
```

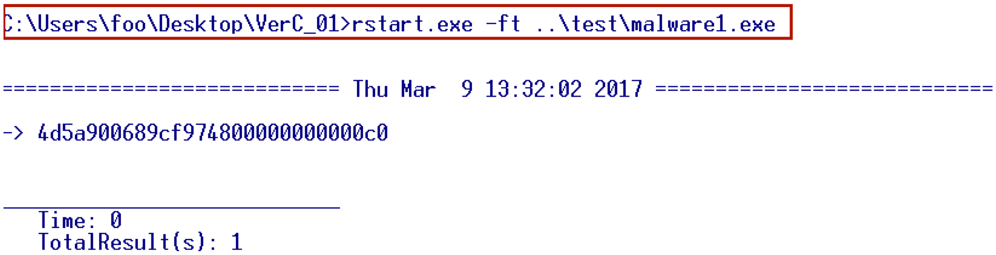
Use case to check file signature with VirusTotal, WildFire or FirEye

```
C:\Users\foo\Desktop\VerC_01>rstart.exe -vd ..\test\malware1.exe

        8b5041d5af8e09d1c8a713b7d81c2e5a        [Malware]

============================ Thu Mar  9 13:30:01 2017 ============================


____________________________
   Time: 2
   TotalResult(s): 0
```

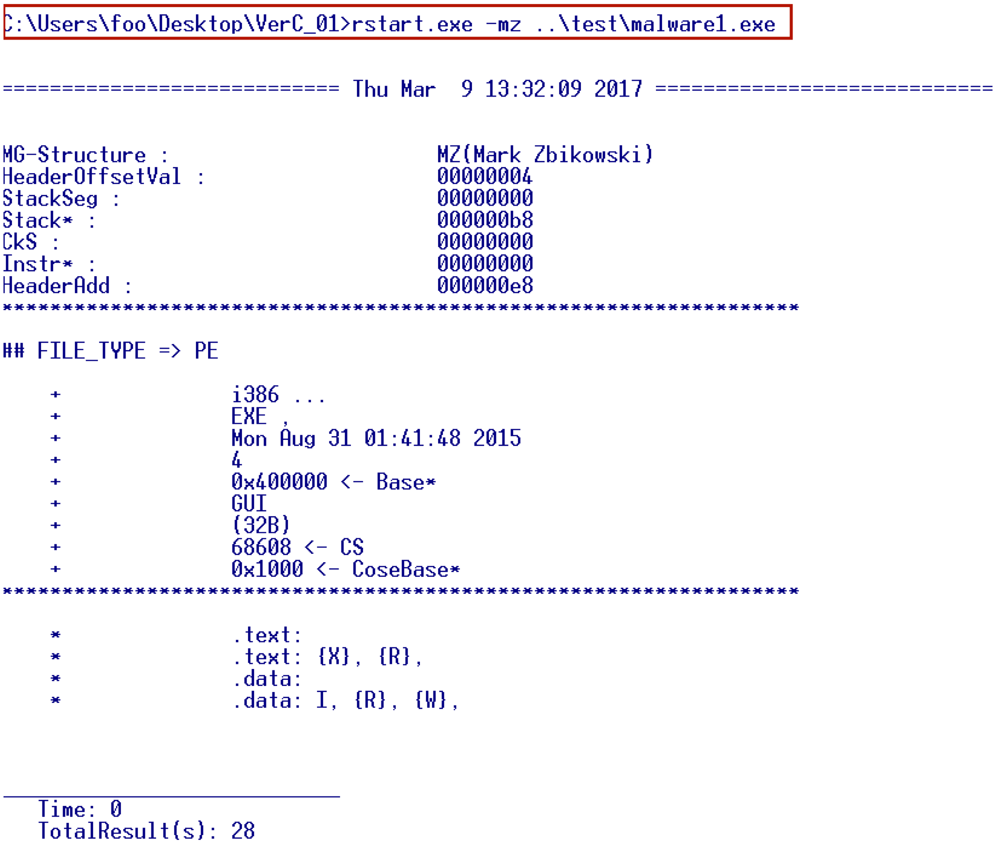
Use case to get information for a binary file

-ft = just the RAW header

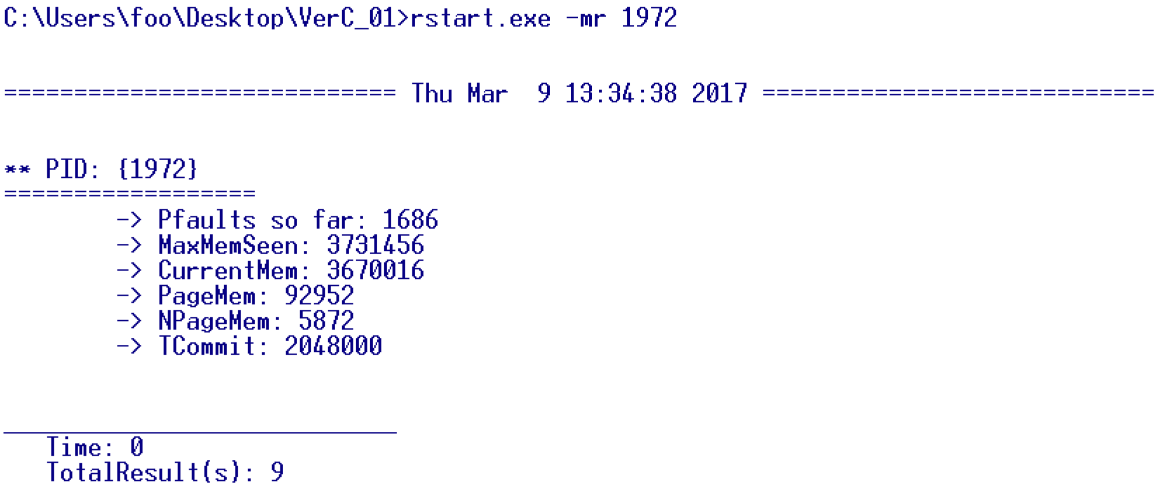
-mz = Verbose info



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -ft ..\test\malware1.exe

============================= Thu Mar  9 13:32:02 2017 =============================

-> 4d5a900689cf9748000000000000c0


_____________________________
   Time: 0
   TotalResult(s): 1
```



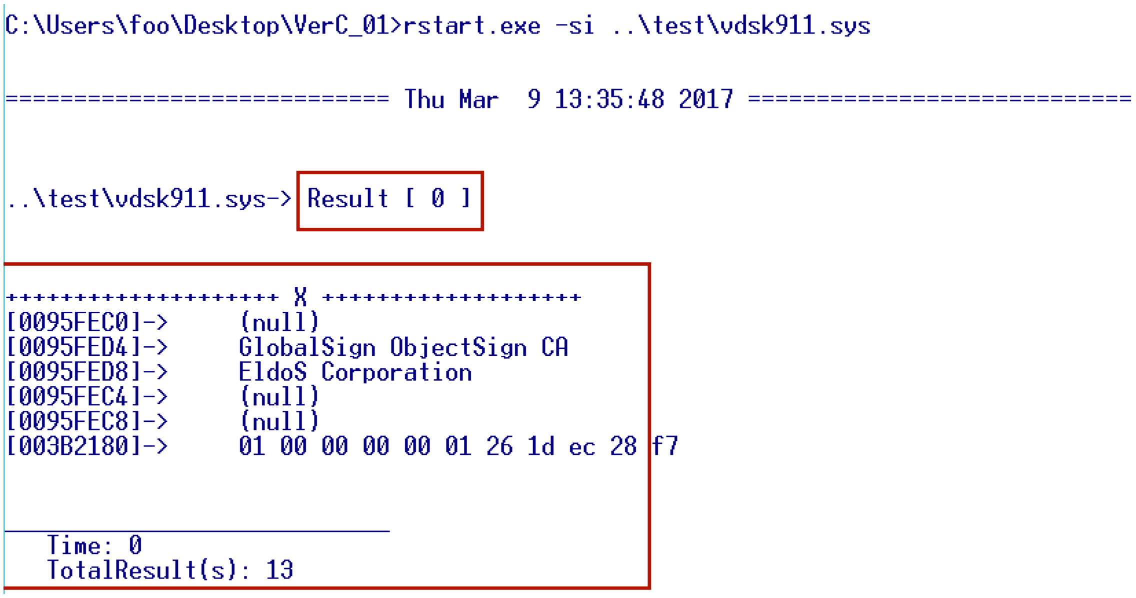
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -mz ..\test\malware1.exe

============================= Thu Mar  9 13:32:09 2017 =============================


MG-Structure :                       MZ(Mark Zbikowski)
HeaderOffsetVal :                    00000004
StackSeg :                           00000000
Stack* :                             000000b8
CkS :                                00000000
Instr* :                             00000000
HeaderAdd :                          000000e8
********************************************************************

## FILE_TYPE => PE

    +              i386 ...
    +              EXE  ,
    +              Mon Aug 31 01:41:48 2015
    +              4
    +              0x400000 <- Base*
    +              GUI
    +              (32B)
    +              68608 <- CS
    +              0x1000 <- CoseBase*
********************************************************************

    *              .text:
    *              .text: {X}, {R},
    *              .data:
    *              .data: I, {R}, {W},



_____________________________
   Time: 0
   TotalResult(s): 28
```



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -mr 1972


============================= Thu Mar  9 13:34:38 2017 =============================


** PID: {1972}
==================
        -> Pfaults so far: 1686
        -> MaxMemSeen: 3731456
        -> CurrentMem: 3670016
        -> PageMem: 92952
        -> NPageMem: 5872
        -> TCommit: 2048000


_____________________________
   Time: 0
   TotalResult(s): 9
```

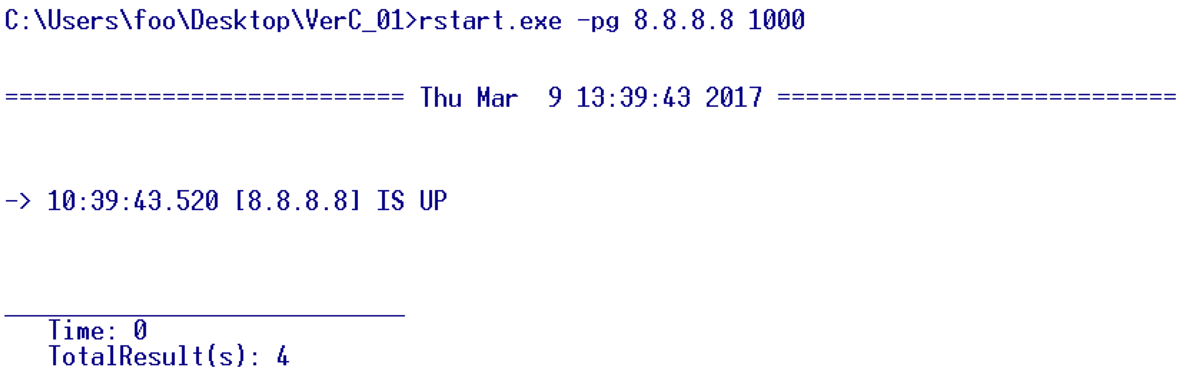
Use case to find binary file signature. Let’s examine Shamoon driver file

Result [0] = Valid signer, -1 = unsigned



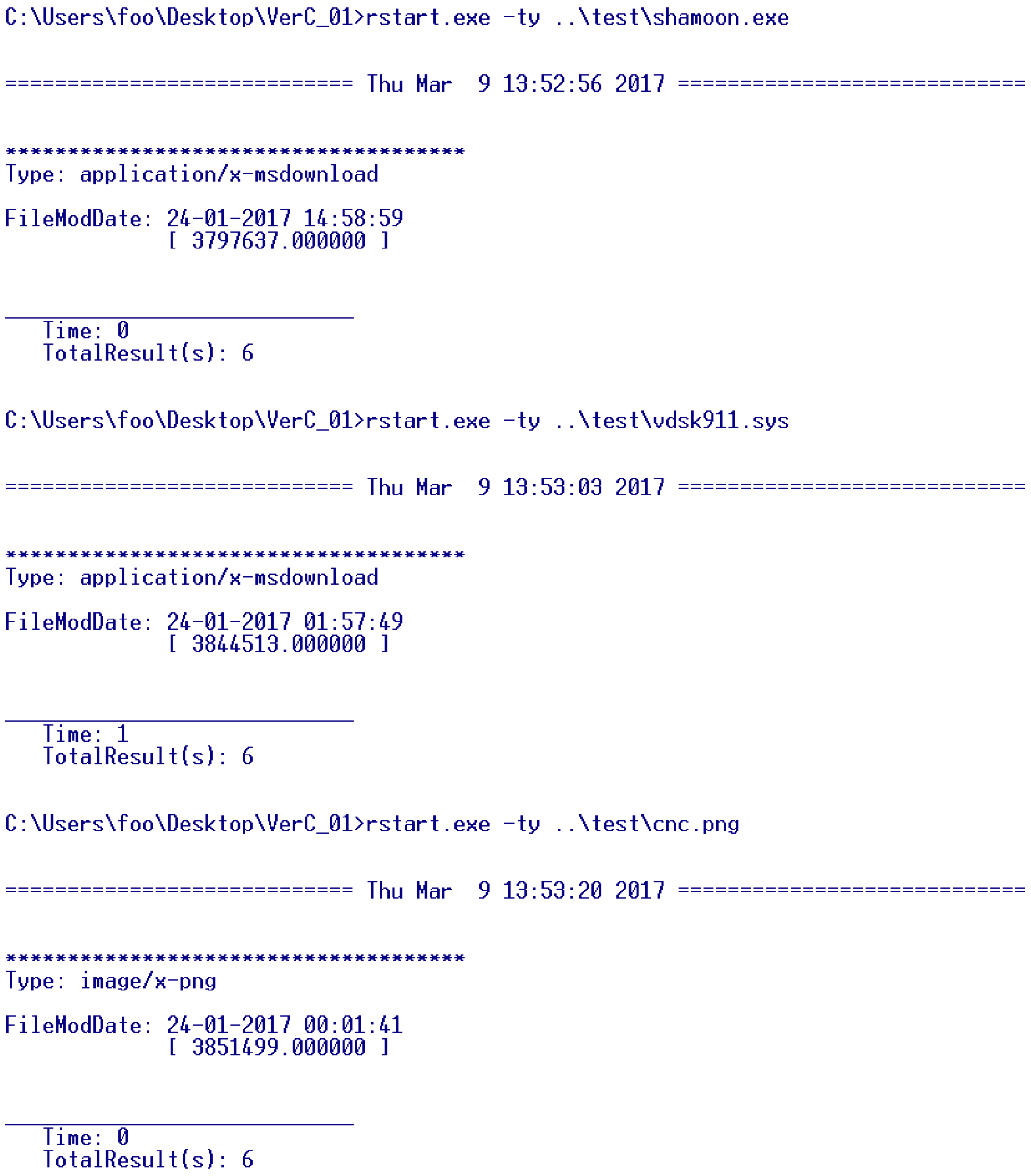
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -si ..\test\vdsk911.sys

============================ Thu Mar  9 13:35:48 2017 ============================


..\test\vdsk911.sys-> Result [ 0 ]

++++++++++++++++++++ X +++++++++++++++++++
[0095FEC0]->     (null)
[0095FED4]->     GlobalSign ObjectSign CA
[0095FED8]->     EldoS Corporation
[0095FEC4]->     (null)
[0095FEC8]->     (null)
[003B2180]->     01 00 00 00 00 01 26 1d ec 28 f7


____________________________
   Time: 0
   TotalResult(s): 13
```

Use case to ping an ip address: This process is extremely fast and user could script it to scan multiple ip’s very quickly. I am adding multi threaded support to this one for multiple ip’s. it requires the ip address and timeout (MilliSeconds)



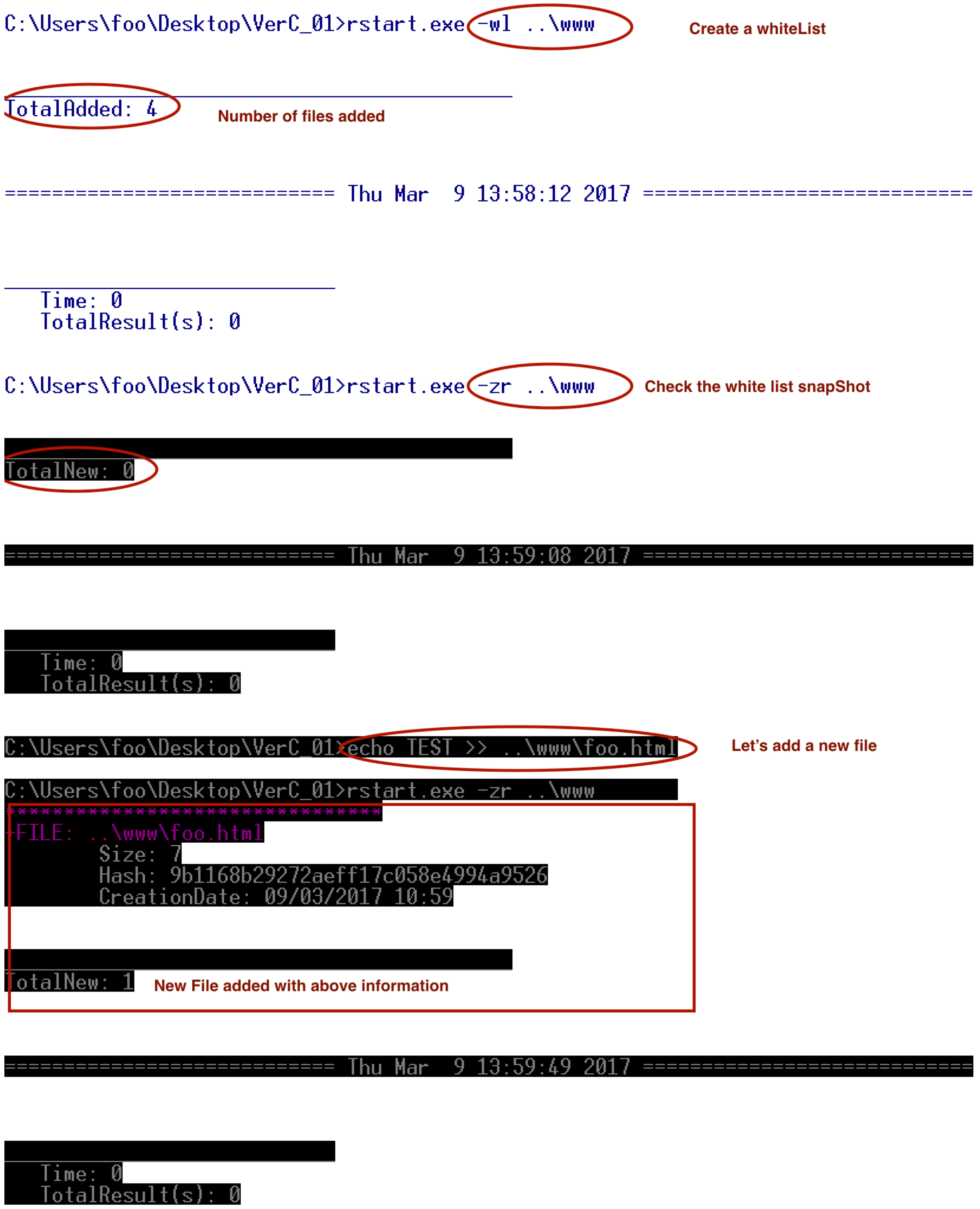
```
C:\Users\foo\Desktop\VerC_01>rstart.exe -pg 8.8.8.8 1000

============================ Thu Mar  9 13:39:43 2017 ============================


-> 10:39:43.520 [8.8.8.8] IS UP



____________________________
   Time: 0
   TotalResult(s): 4
```

Use case to find file type AKA magic:



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -ty ..\test\shamoon.exe

============================ Thu Mar  9 13:52:56 2017 ============================

*************************************
Type: application/x-msdownload

FileModDate: 24-01-2017 14:58:59
             [ 3797637.000000 ]


____________________________
   Time: 0
   TotalResult(s): 6

C:\Users\foo\Desktop\VerC_01>rstart.exe -ty ..\test\vdsk911.sys

============================ Thu Mar  9 13:53:03 2017 ============================

*************************************
Type: application/x-msdownload

FileModDate: 24-01-2017 01:57:49
             [ 3844513.000000 ]


____________________________
   Time: 1
   TotalResult(s): 6

C:\Users\foo\Desktop\VerC_01>rstart.exe -ty ..\test\cnc.png

============================ Thu Mar  9 13:53:20 2017 ============================

*************************************
Type: image/x-png

FileModDate: 24-01-2017 00:01:41
             [ 3851499.000000 ]


____________________________
   Time: 0
   TotalResult(s): 6
```

Use case to take a snap shot of a folder and then compare. This could be used to identify if any new files or folders were added.



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -wl ..\www

TotalAdded: 4

=========================== Thu Mar  9 13:58:12 2017 ===========================


   Time: 0
   TotalResult(s): 0

C:\Users\foo\Desktop\VerC_01>rstart.exe -zr ..\www

TotalNew: 0

=========================== Thu Mar  9 13:59:08 2017 ===========================


   Time: 0
   TotalResult(s): 0

C:\Users\foo\Desktop\VerC_01>echo TEST >> ..\www\foo.html

C:\Users\foo\Desktop\VerC_01>rstart.exe -zr ..\www
*********************************
+FILE: ..\www\foo.html
        Size: 7
        Hash: 9b1168b29272aeff17c058e4994a9526
        CreationDate: 09/03/2017 10:59


TotalNew: 1

=========================== Thu Mar  9 13:59:49 2017 ===========================


   Time: 0
   TotalResult(s): 0
```

Create a whiteList

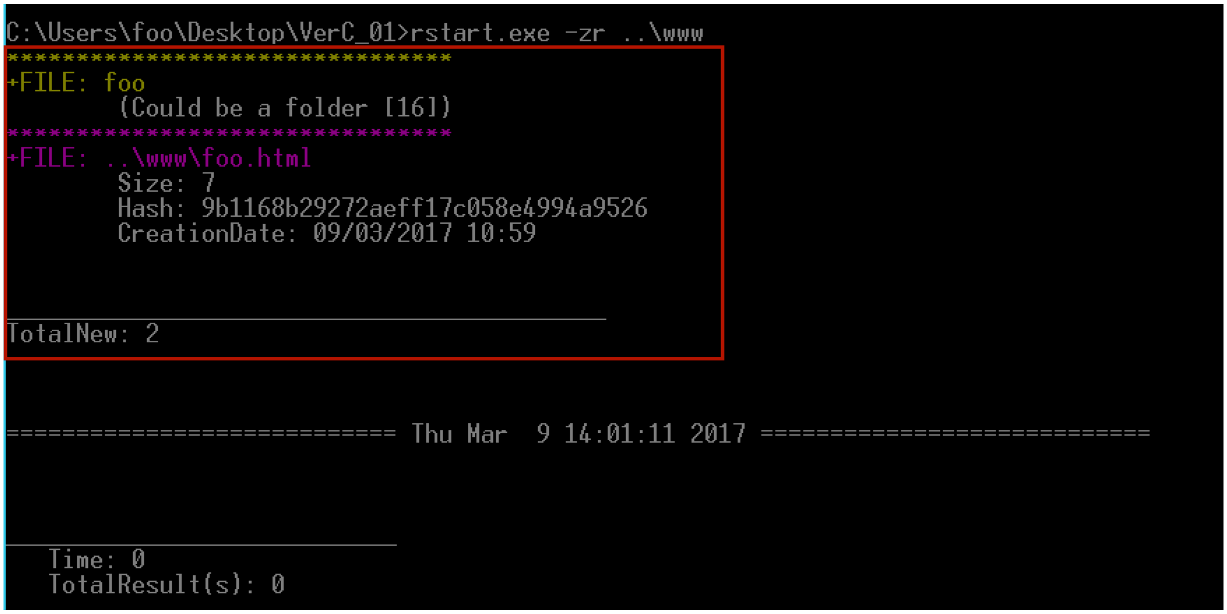
Number of files added

Check the white list snapShot

Let's add a new file

New File added with above information

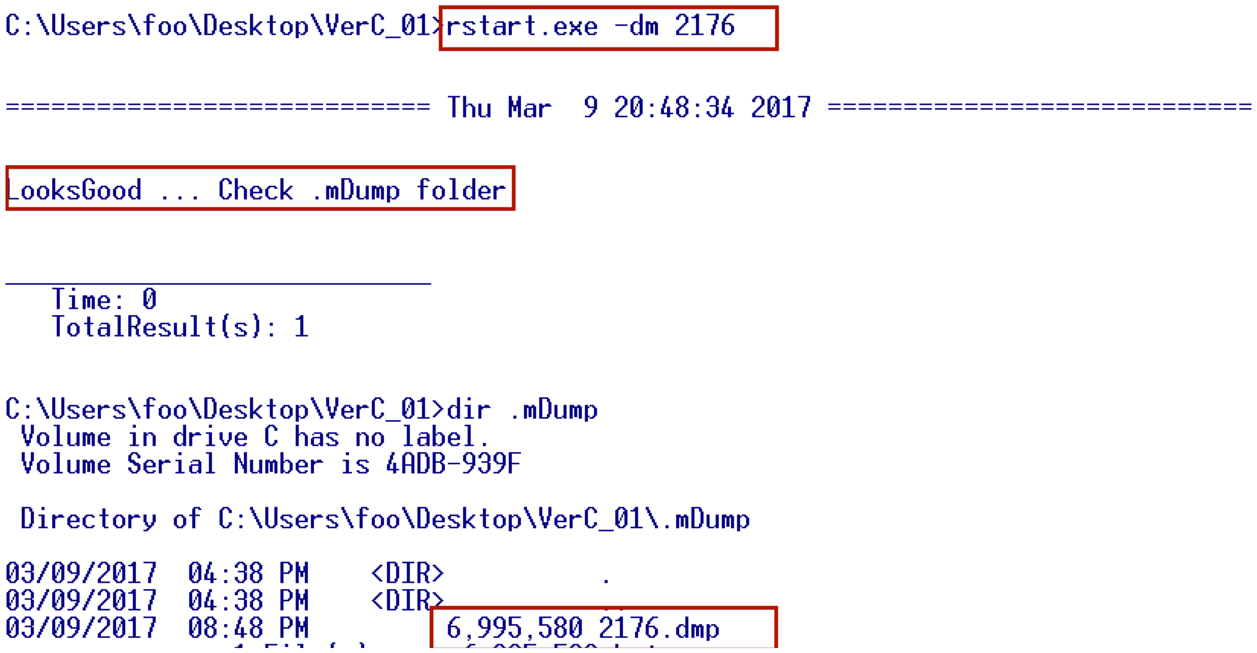
Let's add a new folder and re-run the comparison:



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -zr ..\www
*********************************
+FILE: foo
        (Could be a folder [16])
*********************************
+FILE: ..\www\foo.html
        Size: 7
        Hash: 9b1168b29272aeff17c058e4994a9526
        CreationDate: 09/03/2017 10:59


____________________________________________
TotalNew: 2


============================ Thu Mar  9 14:01:11 2017 ============================



____________________________
   Time: 0
   TotalResult(s): 0
```

Change in size / hash would also alert

Use case to create a memory Dump:



```
C:\Users\foo\Desktop\VerC_01>rstart.exe -dm 2176

============================ Thu Mar  9 20:48:34 2017 ============================

LooksGood ... Check .mDump folder

____________________________
   Time: 0
   TotalResult(s): 1

C:\Users\foo\Desktop\VerC_01>dir .mDump
 Volume in drive C has no label.
 Volume Serial Number is 4ADB-939F

 Directory of C:\Users\foo\Desktop\VerC_01\.mDump

03/09/2017  04:38 PM    <DIR>          .
03/09/2017  04:38 PM    <DIR>          ..
03/09/2017  08:48 PM         6,995,580 2176.dmp
```