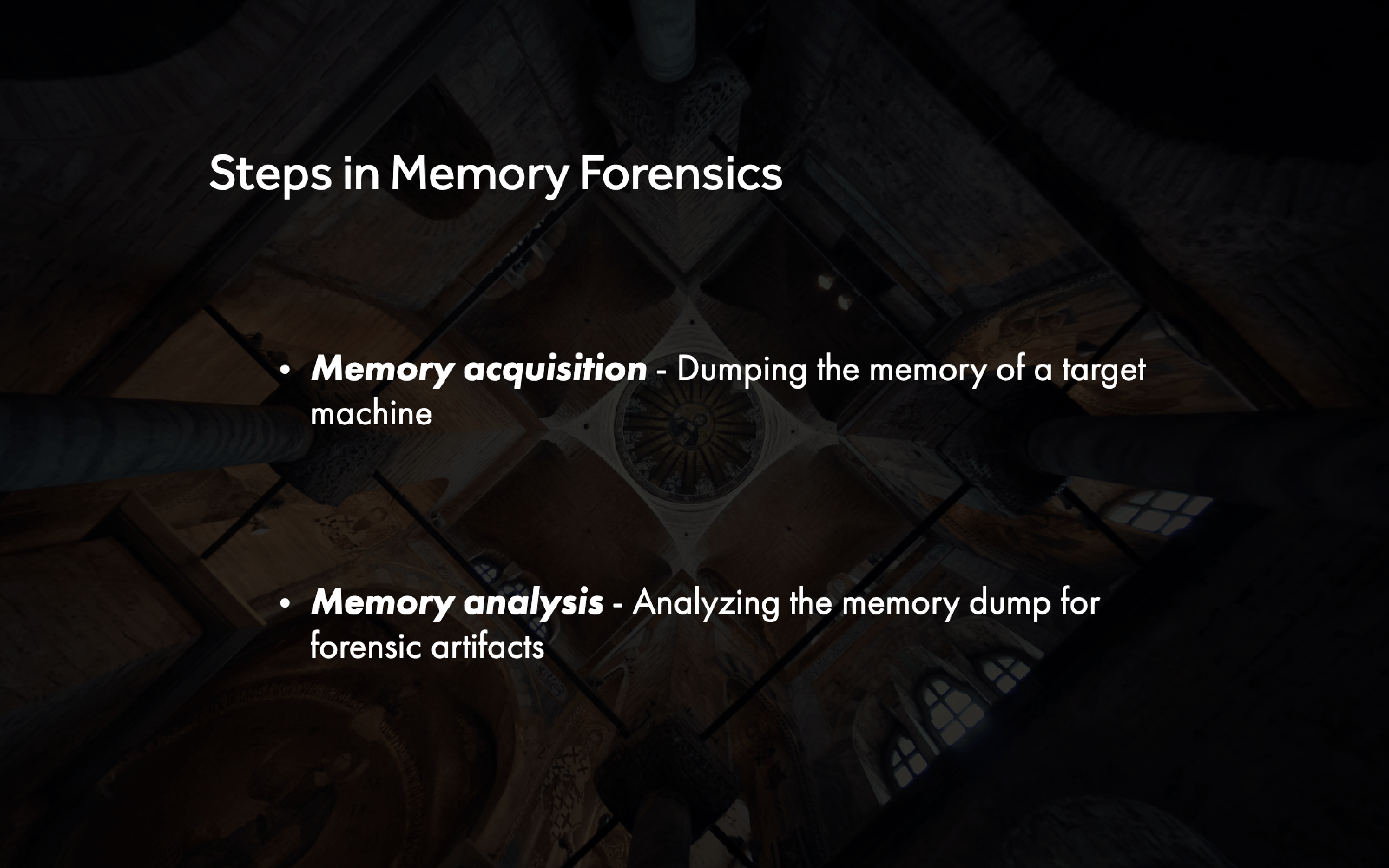
Introduction to Memory Forensics

Why Memory Forensics?

- Finding and extracting forensic artifacts
- Helps in malware analysis
- Determining process, network, registry activities
- Reconstructing the original state of the system
- Assists with unpacking, rootkit detection, and reverse engineering
- Sophisticated actors
- Critical data exists in memory



Steps in Memory Forensics

- ***Memory acquisition*** - Dumping the memory of a target machine
- ***Memory analysis*** - Analyzing the memory dump for forensic artifacts

Memory Acquisition and tools

Process of Acquiring Volatile memory to non volatile storage

On Physical Machines(Tools):

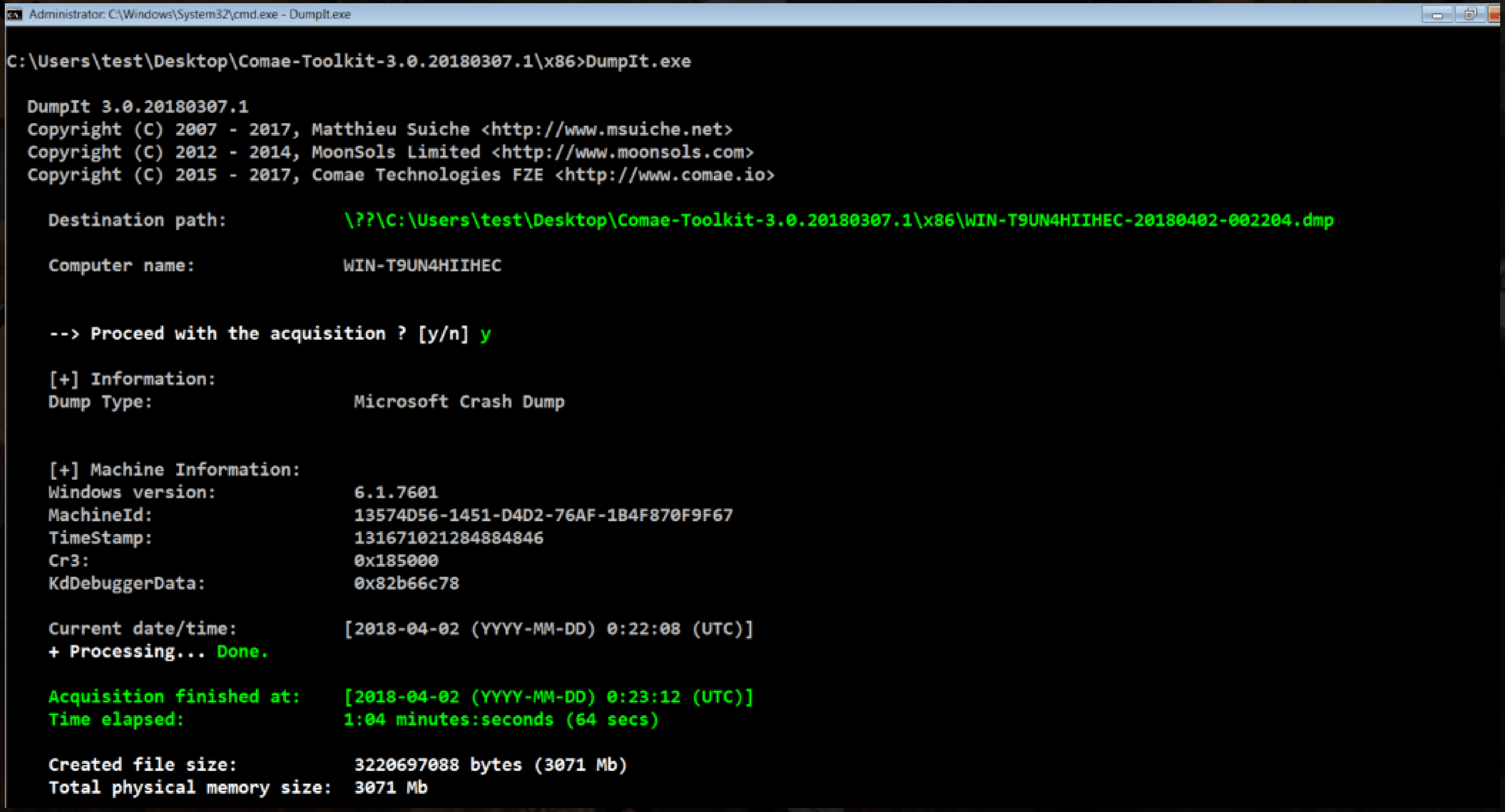
- Comae Memory Toolkit (DumpIt) by Comae Technologies
- Belkasoft RAM Capturer
- Mandiant Memoryze
- HBGary FastDump
- KnTTools
- FTK Imager by AccessData

On Virtual Machines:

- Suspend the VM (.vmem)

Acquiring memory from the Physical machine

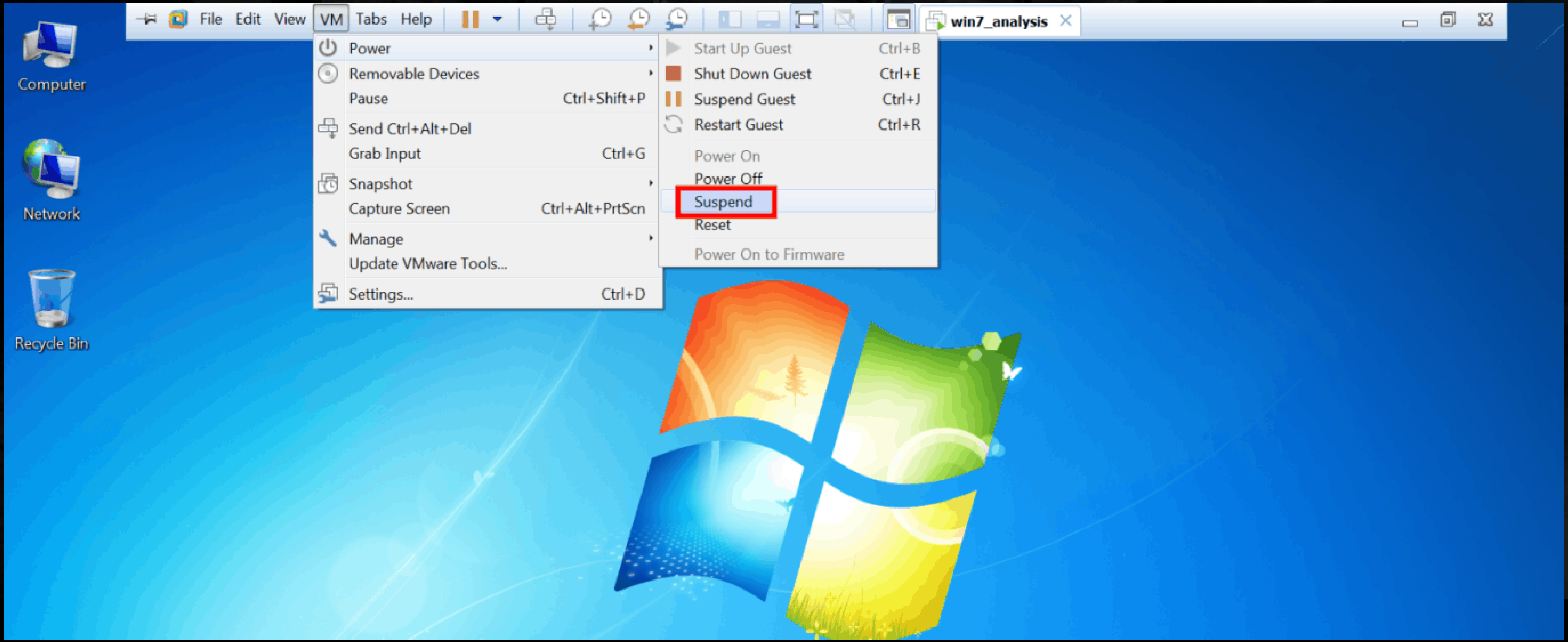
Open ***cmd.exe*** with admin privileges and run ***Dumpit.exe***. By default, DumpIt dumps the memory to a file as Microsoft Crash Dump (with ***.dm***p extension)



```
C:\Users\test\Desktop\Comae-Toolkit-3.0.20180307.1\x86>DumpIt.exe

  DumpIt 3.0.20180307.1
  Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
  Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
  Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

    Destination path:           \??\C:\Users\test\Desktop\Comae-Toolkit-3.0.20180307.1\x86\WIN-T9UN4HIIHEC-20180402-002204.dmp

    Computer name:              WIN-T9UN4HIIHEC


    --> Proceed with the acquisition ? [y/n] y

    [+] Information:
    Dump Type:                   Microsoft Crash Dump


    [+] Machine Information:
    Windows version:             6.1.7601
    MachineId:                   13574D56-1451-D4D2-76AF-1B4F870F9F67
    TimeStamp:                   131671021284884846
    Cr3:                         0x185000
    KdDebuggerData:              0x82b66c78

    Current date/time:          [2018-04-02 (YYYY-MM-DD) 0:22:08 (UTC)]
    + Processing... Done.

    Acquisition finished at:    [2018-04-02 (YYYY-MM-DD) 0:23:12 (UTC)]
    Time elapsed:               1:04 minutes:seconds (64 secs)

    Created file size:           3220697088 bytes (3071 Mb)
    Total physical memory size:  3071 Mb
```

Acquiring Memory from Virtual Machine

Suspending the virtual machine creates a file with the ***.vmem*** extension, that is the memory image


File
Edit
View
VM
Tabs
Help
win7_analysis
Power
Removable Devices
Pause Ctrl+Shift+P
Send Ctrl+Alt+Del
Grab Input Ctrl+G
Snapshot
Capture Screen Ctrl+Alt+PrtScn
Manage
Update VMware Tools...
Settings... Ctrl+D
Start Up Guest Ctrl+B
Shut Down Guest Ctrl+E
Suspend Guest Ctrl+J
Restart Guest Ctrl+R
Power On
Power Off
Suspend
Reset
Power On to Firmware
Computer
Network
Recycle Bin