Computer & Network Forensics

Week 2 (Lab1)

Software Write-Blocker

Questions

1. Why are write blockers essential in a forensics investigation?

   Write blockers are very important in digital forensics because this basically protects the original evidence. When investigators plug in a suspect's hard drive or USB, we need to look at everything on it without accidentally changing a single thing. Even something small, like the system updating a file timestamp, could mess up the case and make evidence unusable in court. Write blockers stop the computer from writing anything back to the device, so investigators can safely read the data without worrying about altering it.

2. What are the main types of write blockers?

   There are two main types: hardware and software. Hardware write blockers are physical devices you plug the suspect's drive into before connecting it to the forensic machine; they block all writes at the hardware level. Software write blockers are programs that run on the computer to stop write commands.

3. What are the main challenges of write blocking for forensics investigators?

   One challenge is compatibility – some drives or file systems don't play nice with certain write blockers. Another issue is reliability: investigators need to be absolutely sure the blocker is actually preventing writes, because if something slips through, the evidence could be compromised. There's also the cost factor, since good hardware blockers can be expensive. Plus, investigators need to stay updated with technology changes – new storage devices come out all the time, and blockers need to keep up.

4. Discuss the implications of using open-source technologies for write blocking.

   Open-source tools are appealing because they're free and customizable, but they also come with risks. Since the code is public, it can be inspected for flaws, which is good for transparency. But at the same time, it might not always meet strict forensic standards, and defense lawyers could challenge its reliability in court. Also, open-source tools often don't get the same level of official certification as commercial hardware blockers. So, while open-source can be great for learning or smaller cases, most professionals stick with certified tools when they know evidence might go to trial.

Computer & Network Forensics

Week 2 (Lab1a)

Extracting Volatile Data (Manually)

Commands

1. Command to Capture System Information

   ```
   systeminfo >> VolatileDataFile.txt
   ```
   → Capture the system information and save it into a text file for later analysis

2. Checking Active Network Connections

   ```
   netstat -nao >> VolatileDataFile.txt
   ```
   → Using the netstat (network statistics) command, we can capture details about all active network connections

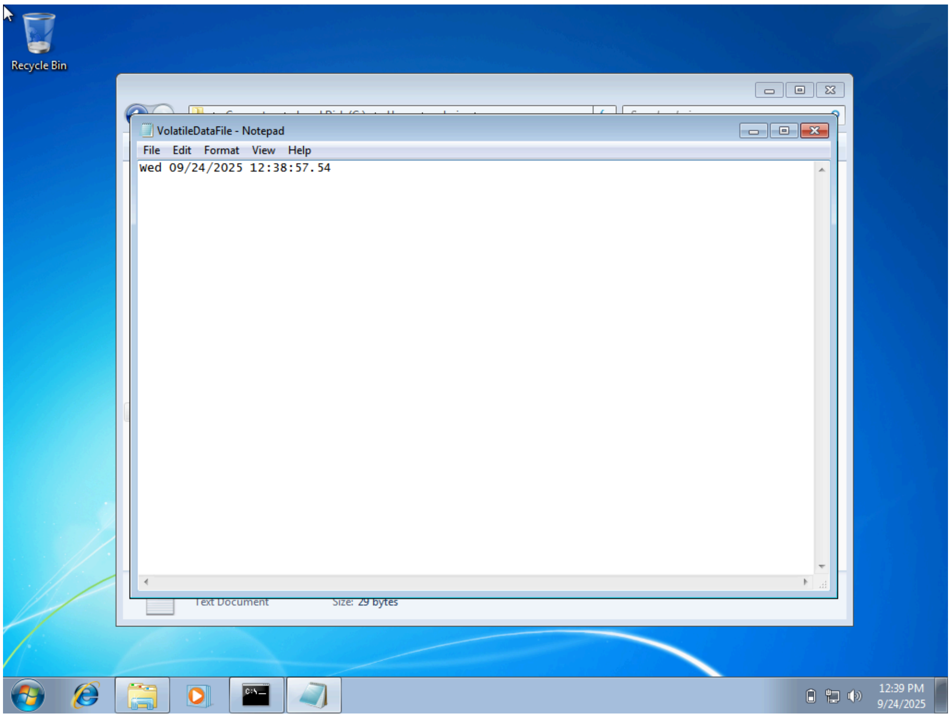
3. Routing Configuration

   ```
   route print >> VolatileDataFile.txt
   ```
   → Routing configuration refers to the setup of IP addresses, gateway settings, and network routes that direct data traffic between devices in a network. This information is crucial in digital forensics because improper or malicious routing could indicate unauthorized access or a compromised system.

1. Date and Time

```
echo %date% %time% > VolatileDataFile.txt
```

→ Records the current system date and time. Useful for timestamping forensic collection.

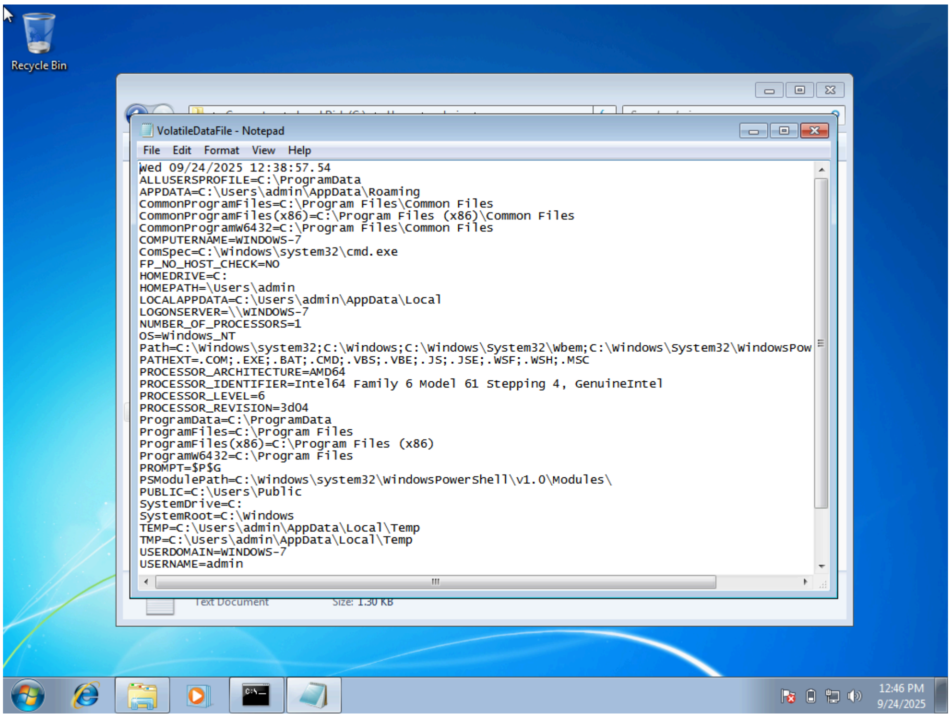


```
Wed 09/24/2025 12:38:57.54
```

2. System Variables

```
set >> VolatileDataFile.txt
```

→ Lists all environment variables. Helps investigators see system paths, user variables, and possible malware persistence points.

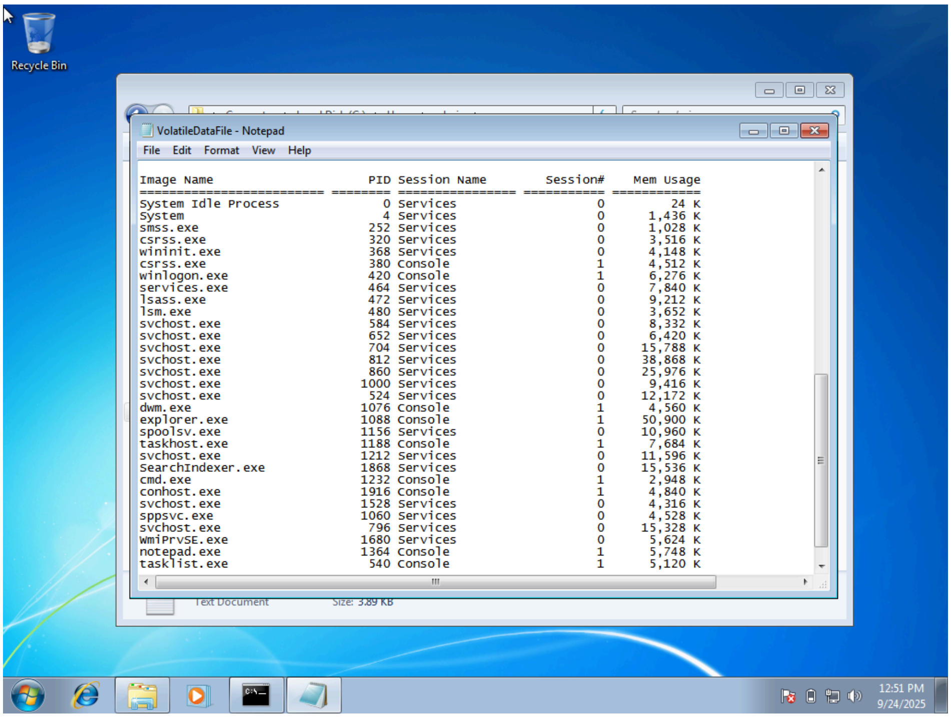


```
Wed 09/24/2025 12:38:57.54
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\admin\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=WINDOWS-7
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\admin
LOCALAPPDATA=C:\Users\admin\AppData\Local
LOGONSERVER=\\WINDOWS-7
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPow
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 61 Stepping 4, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3d04
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\admin\AppData\Local\Temp
TMP=C:\Users\admin\AppData\Local\Temp
USERDOMAIN=WINDOWS-7
USERNAME=admin
```

3. Task List

```
tasklist >> VolatileDataFile.txt
```

→ Shows all running processes with PID and memory usage. Detects suspicious programs.

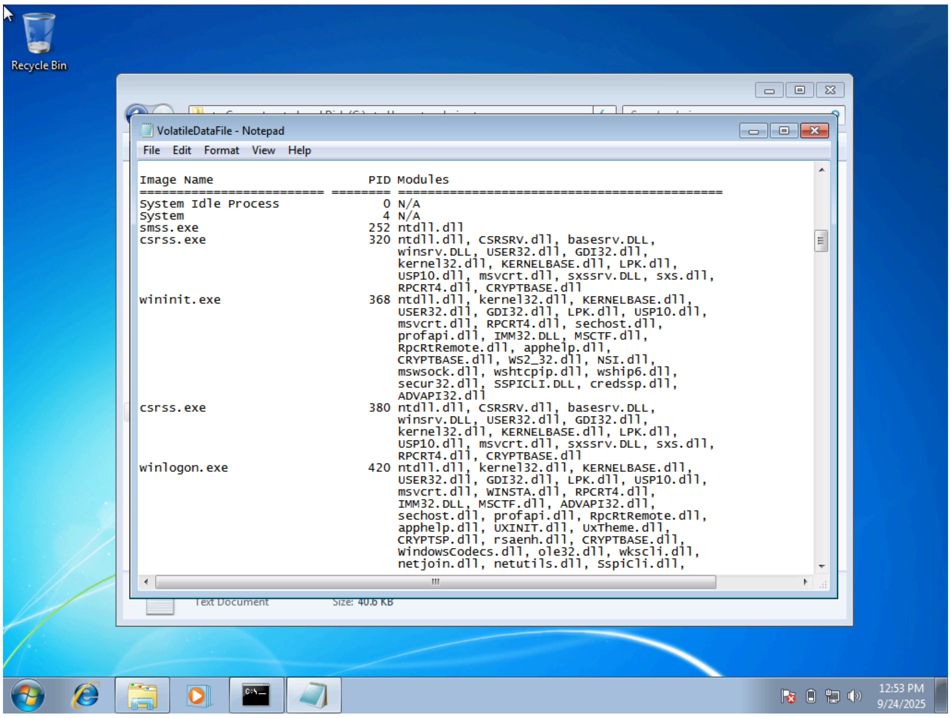


```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      1,436 K
smss.exe                       252 Services                   0      1,028 K
csrss.exe                      320 Services                   0      3,516 K
wininit.exe                    368 Services                   0      4,148 K
csrss.exe                      380 Console                    1      4,512 K
winlogon.exe                   420 Console                    1      6,276 K
services.exe                   464 Services                   0      7,840 K
lsass.exe                      472 Services                   0      9,212 K
lsm.exe                        480 Services                   0      3,652 K
svchost.exe                    584 Services                   0      8,332 K
svchost.exe                    652 Services                   0      6,420 K
svchost.exe                    704 Services                   0     15,788 K
svchost.exe                    812 Services                   0     38,868 K
svchost.exe                    860 Services                   0     25,976 K
svchost.exe                   1000 Services                   0      9,416 K
svchost.exe                    524 Services                   0     12,172 K
dwm.exe                       1076 Console                    1      4,560 K
explorer.exe                  1088 Console                    1     50,900 K
spoolsv.exe                   1156 Services                   0     10,960 K
taskhost.exe                  1188 Console                    1      7,684 K
svchost.exe                   1212 Services                   0     11,596 K
SearchIndexer.exe             1868 Services                   0     15,536 K
cmd.exe                       1232 Console                    1      2,948 K
conhost.exe                   1916 Console                    1      4,840 K
svchost.exe                   1528 Services                   0      4,316 K
sppsvc.exe                    1060 Services                   0      4,528 K
svchost.exe                    796 Services                   0     15,328 K
WmiPrvSE.exe                  1680 Services                   0      5,624 K
notepad.exe                   1364 Console                    1      5,748 K
tasklist.exe                   540 Console                    1      5,120 K
```

4. Task List with Modules

```
tasklist /m >> VolatileDataFile.txt
```

→ Shows processes with loaded DLL modules. Can reveal injected malicious DLLs.

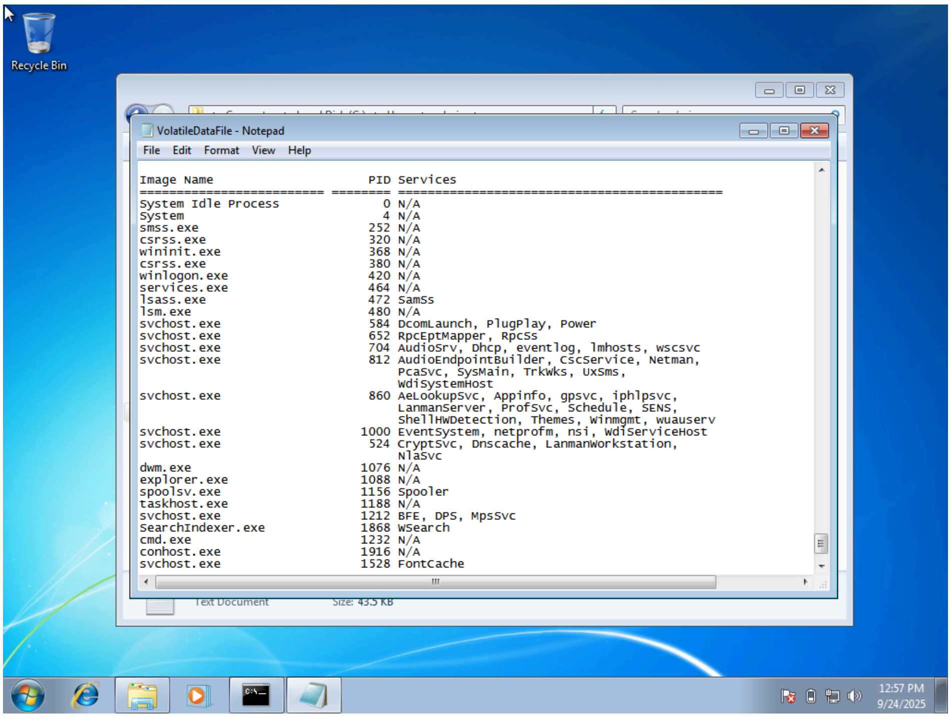


```
Image Name                     PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       252 ntdll.dll
csrss.exe                      320 ntdll.dll, CSRSRV.dll, basesrv.DLL,
                                   winsrv.DLL, USER32.dll, GDI32.dll,
                                   kernel32.dll, KERNELBASE.dll, LPK.dll,
                                   USP10.dll, msvcrt.dll, sxssrv.DLL, sxs.dll,
                                   RPCRT4.dll, CRYPTBASE.dll
wininit.exe                    368 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
                                   msvcrt.dll, RPCRT4.dll, sechost.dll,
                                   profapi.dll, IMM32.DLL, MSCTF.dll,
                                   RpcRtRemote.dll, apphelp.dll,
                                   CRYPTBASE.dll, WS2_32.dll, NSI.dll,
                                   mswsock.dll, wshtcpip.dll, wship6.dll,
                                   secur32.dll, SSPICLI.DLL, credssp.dll,
                                   ADVAPI32.dll
csrss.exe                      380 ntdll.dll, CSRSRV.dll, basesrv.DLL,
                                   winsrv.DLL, USER32.dll, GDI32.dll,
                                   kernel32.dll, KERNELBASE.dll, LPK.dll,
                                   USP10.dll, msvcrt.dll, sxssrv.DLL, sxs.dll,
                                   RPCRT4.dll, CRYPTBASE.dll
winlogon.exe                   420 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
                                   msvcrt.dll, WINSTA.dll, RPCRT4.dll,
                                   IMM32.DLL, MSCTF.dll, ADVAPI32.dll,
                                   sechost.dll, profapi.dll, RpcRtRemote.dll,
                                   apphelp.dll, UXINIT.dll, UxTheme.dll,
                                   CRYPTSP.dll, rsaenh.dll, CRYPTBASE.dll,
                                   WindowsCodecs.dll, ole32.dll, wkscli.dll,
                                   netjoin.dll, netutils.dll, SspiCli.dll,
```

5. Task List with Services

```
tasklist /svc >> VolatileDataFile.txt
```

→ Links processes to services they host. Useful for spotting rogue services.

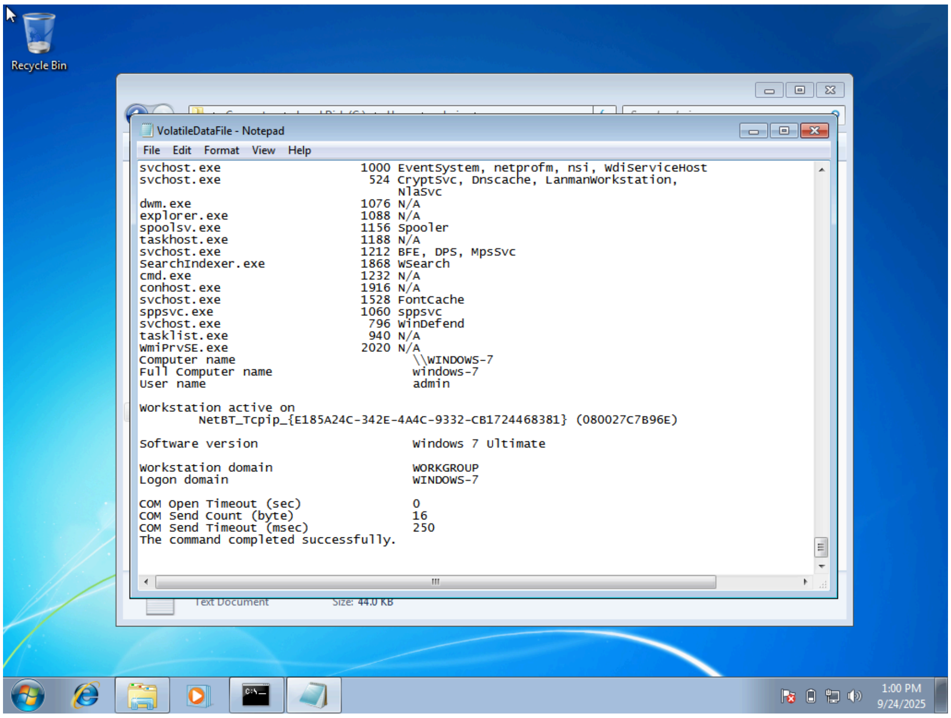


```
Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       252 N/A
csrss.exe                      320 N/A
wininit.exe                    368 N/A
csrss.exe                      380 N/A
winlogon.exe                   420 N/A
services.exe                   464 N/A
lsass.exe                      472 SamSs
lsm.exe                        480 N/A
svchost.exe                    584 DcomLaunch, PlugPlay, Power
svchost.exe                    652 RpcEptMapper, RpcSs
svchost.exe                    704 AudioSrv, Dhcp, eventlog, lmhosts, wscsvc
svchost.exe                    812 AudioEndpointBuilder, CscService, Netman,
                                   PcaSvc, SysMain, TrkWks, UxSms,
                                   WdiSystemHost
svchost.exe                    860 AeLookupSvc, Appinfo, gpsvc, iphlpsvc,
                                   LanmanServer, ProfSvc, Schedule, SENS,
                                   ShellHWDetection, Themes, Winmgmt, wuauserv
svchost.exe                   1000 EventSystem, netprofm, nsi, WdiServiceHost
svchost.exe                    524 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc
dwm.exe                       1076 N/A
explorer.exe                  1088 N/A
spoolsv.exe                   1156 Spooler
taskhost.exe                  1188 N/A
svchost.exe                   1212 BFE, DPS, MpsSvc
SearchIndexer.exe             1868 WSearch
cmd.exe                       1232 N/A
conhost.exe                   1916 N/A
svchost.exe                   1528 FontCache
```

6. Workstation Information

```
net config workstation >> VolatileDataFile.txt
```

→ Displays workstation settings like computer name, domain, and logon details.

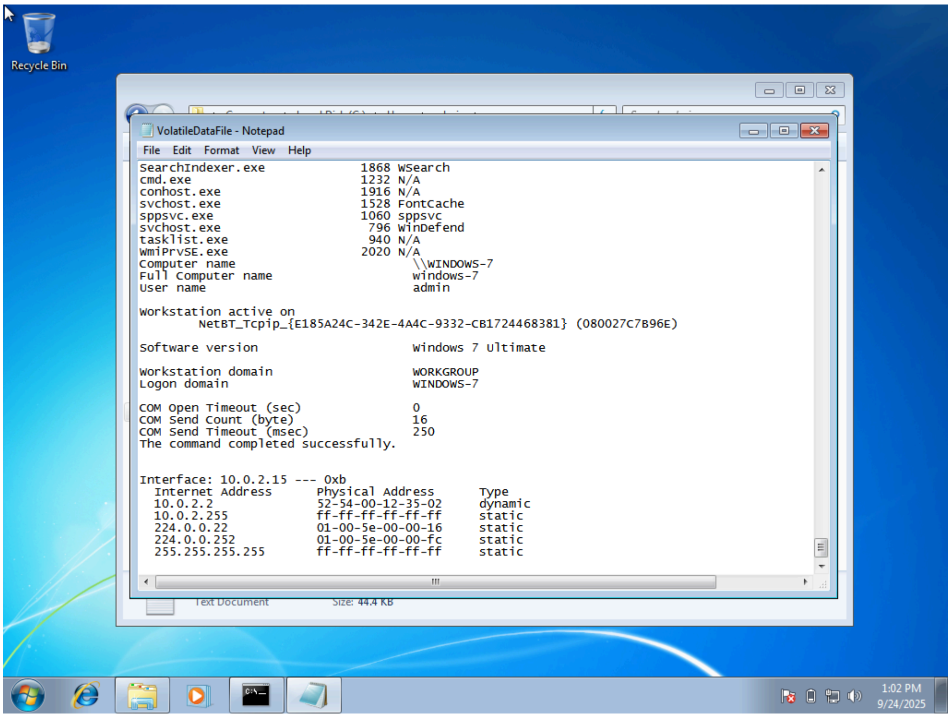


```
svchost.exe                   1000 EventSystem, netprofm, nsi, WdiServiceHost
svchost.exe                    524 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc
dwm.exe                       1076 N/A
explorer.exe                  1088 N/A
spoolsv.exe                   1156 Spooler
taskhost.exe                  1188 N/A
svchost.exe                   1212 BFE, DPS, MpsSvc
SearchIndexer.exe             1868 WSearch
cmd.exe                       1232 N/A
conhost.exe                   1916 N/A
svchost.exe                   1528 FontCache
sppsvc.exe                    1060 sppsvc
svchost.exe                    796 WinDefend
tasklist.exe                   940 N/A
WmiPrvSE.exe                  2020 N/A
Computer name                        \\WINDOWS-7
Full Computer name                   windows-7
User name                            admin

Workstation active on
        NetBT_Tcpip_{E185A24C-342E-4A4C-9332-CB1724468381} (080027C7B96E)

Software version                     Windows 7 Ultimate

Workstation domain                   WORKGROUP
Logon domain                         WINDOWS-7

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.
```

7. MAC Address saved in System ARP Cache

```
arp -a >> VolatileDataFile.txt
```

→ Shows IP-to-MAC address mappings. Helps trace active devices on the local network.

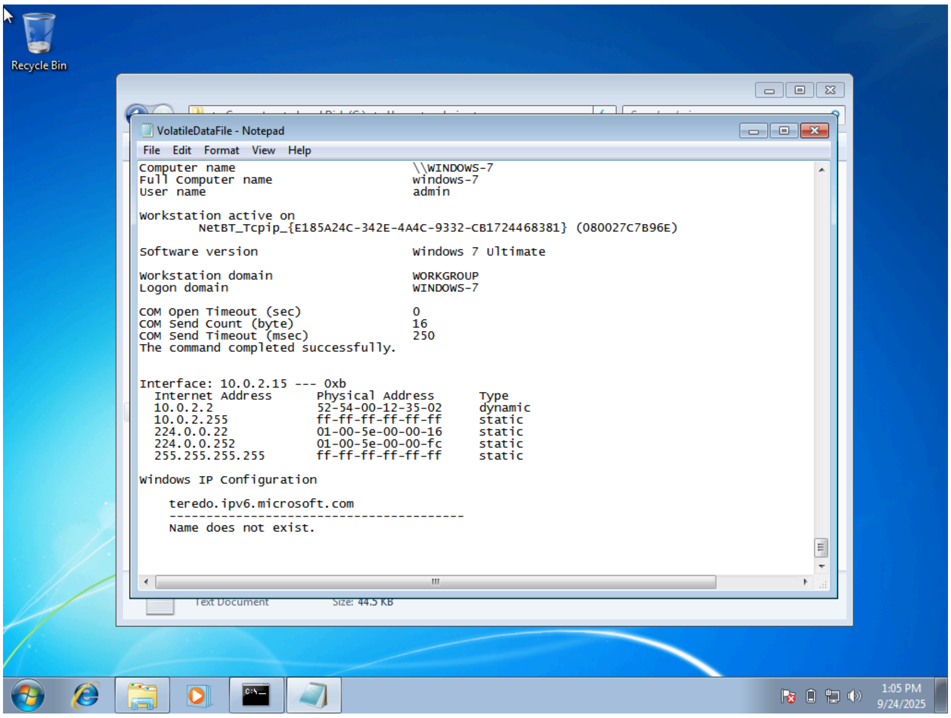


```
SearchIndexer.exe              1868 WSearch
cmd.exe                        1232 N/A
conhost.exe                    1916 N/A
svchost.exe                    1528 FontCache
sppsvc.exe                     1060 sppsvc
svchost.exe                     796 WinDefend
tasklist.exe                    940 N/A
WmiPrvSE.exe                   2020 N/A
Computer name                        \\WINDOWS-7
Full Computer name                   windows-7
User name                            admin

Workstation active on
        NetBT_Tcpip_{E185A24C-342E-4A4C-9332-CB1724468381} (080027C7B96E)

Software version                     Windows 7 Ultimate

Workstation domain                   WORKGROUP
Logon domain                         WINDOWS-7

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

8. DNS Configuration

```
ipconfig /displaydns >> VolatileDataFile.txt
```

→ Lists cached DNS records. Useful for spotting suspicious domains visited.

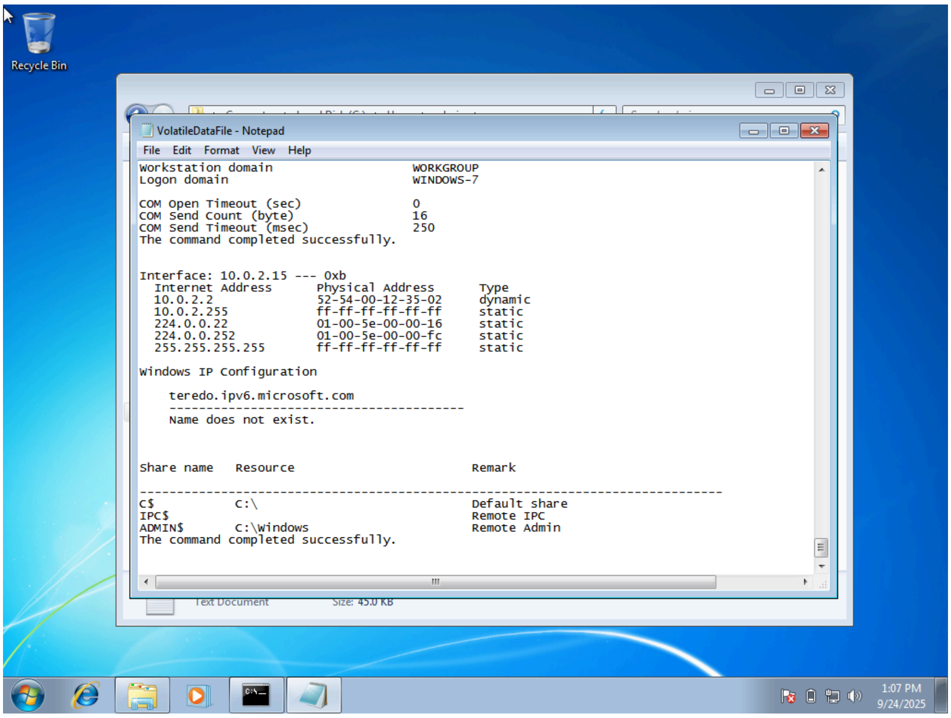


```
Computer name                        \\WINDOWS-7
Full Computer name                   windows-7
User name                            admin

Workstation active on
        NetBT_Tcpip_{E185A24C-342E-4A4C-9332-CB1724468381} (080027C7B96E)

Software version                     Windows 7 Ultimate

Workstation domain                   WORKGROUP
Logon domain                         WINDOWS-7

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Windows IP Configuration

    teredo.ipv6.microsoft.com
    ----------------------------------------
    Name does not exist.
```

9. System network shares

```
net share >> VolatileDataFile.txt
```

→ Displays shared folders. Attackers might create hidden shares for data theft.

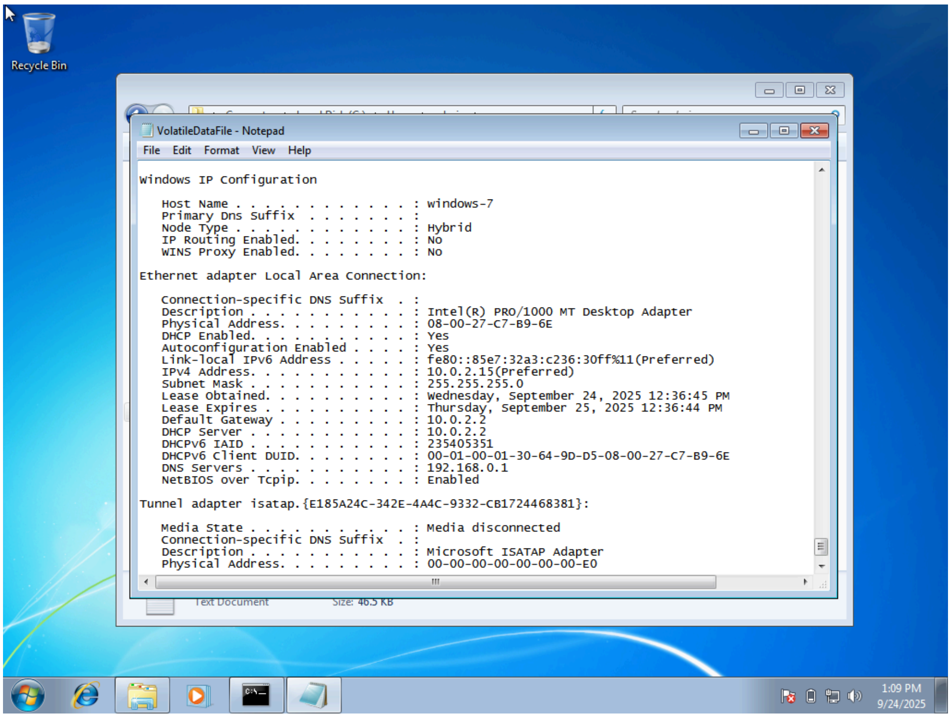


```
Workstation domain                   WORKGROUP
Logon domain                         WINDOWS-7

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Windows IP Configuration

    teredo.ipv6.microsoft.com
    ----------------------------------------
    Name does not exist.



Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.
```

10. Network Configuration

```
ipconfig /all >> VolatileDataFile.txt
```

→ Shows detailed network adapter settings, IPs, gateways, and DNS servers. Can reveal anomalies like rogue DNS or static routes.



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : windows-7
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-C7-B9-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::85e7:32a3:c236:30ff%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 24, 2025 12:36:45 PM
   Lease Expires . . . . . . . . . . : Thursday, September 25, 2025 12:36:44 PM
   Default Gateway . . . . . . . . . : 10.0.2.2
   DHCP Server . . . . . . . . . . . : 10.0.2.2
   DHCPv6 IAID . . . . . . . . . . . : 235405351
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-30-64-9D-D5-08-00-27-C7-B9-6E
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{E185A24C-342E-4A4C-9332-CB1724468381}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
```