

Computer & Network Forensics

Lab 1

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

Lab 1a

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

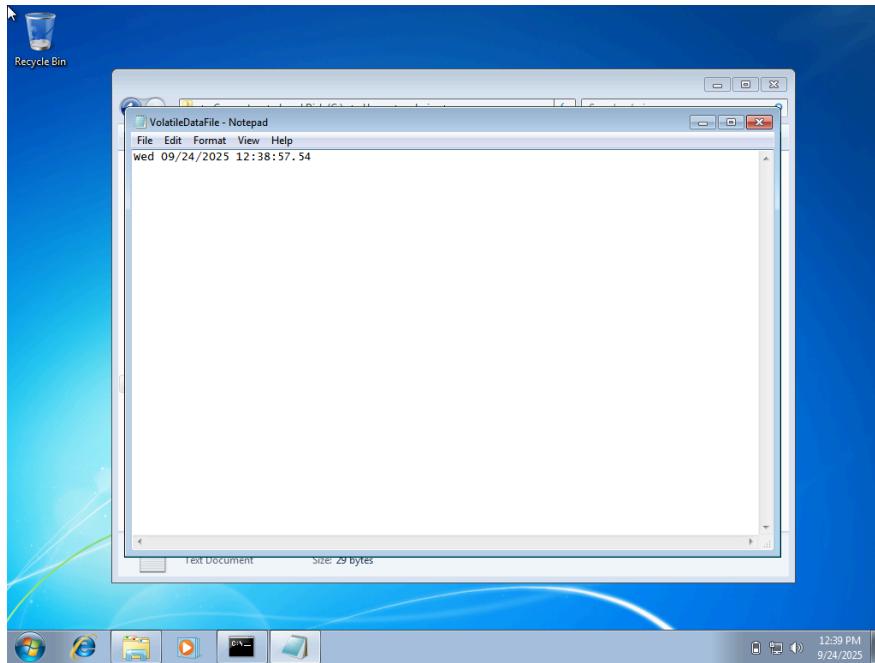
```
route print >> VolatileDataFile.txt
```

→ 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
```

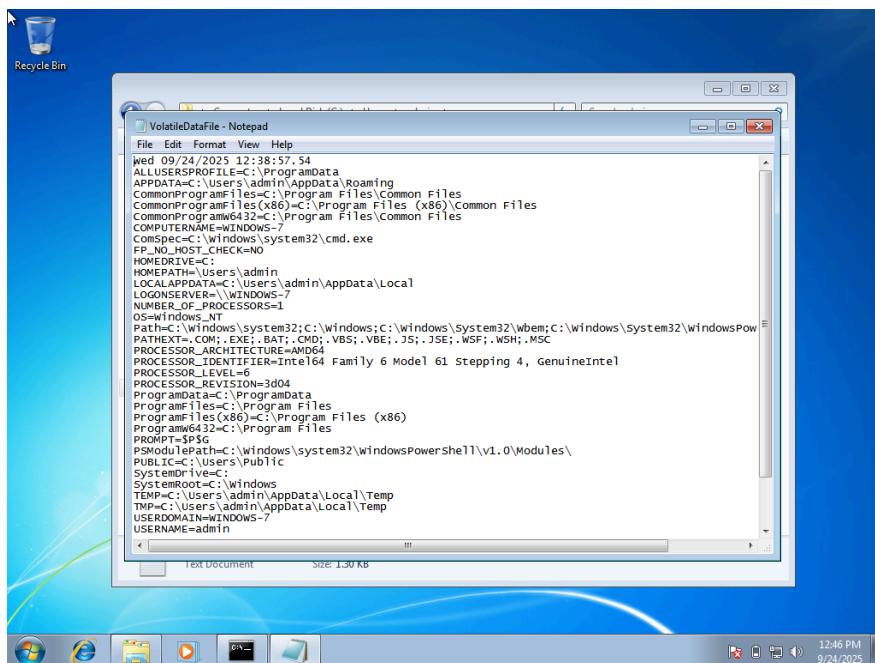
→ Records the current system date and time. Useful for timestamping forensic collection.



2. System Variables

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

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



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	3,732 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	20,976 K
svchost.exe	1000	Services	0	9,16 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
sppsvc.exe	1152	Services	0	10,660 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	2,944 K
compmgmt.msc	1916	Console	1	4,640 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	1284	Console	1	5,148 K
tasklist.exe	540	Console	1	5,120 K

4. Task List with Modules

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

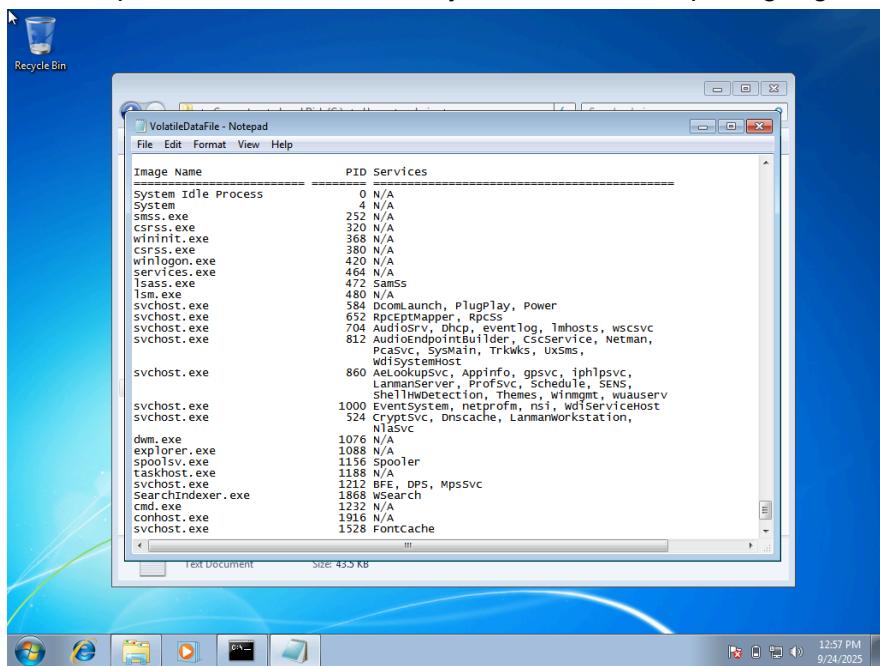
→ Shows processes with loaded DLL modules. Can reveal injected malicious DLLs.

Image Name	PID	Modules
System Idle Process	0	N/A
System	4	N/A
smss.exe	252	ntdll.dll, csrssrv.dll, basesrv.dll,
csrss.exe	320	win32.dll, USER32.dll, GDI32.dll,
		kernel32.dll, KERNELBASE.dll, LPK.dll,
wininit.exe	368	USP10.dll, msvcr.dll, sxssrv.dll, sxs.dll,
		RPCRT4.dll, cryptbase.dll, KERNELBASE.dll,
		USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
		msvcr.dll, RPCRT4.dll, sechost.dll,
		profapi.dll, IMM32.dll, MSCTF.dll,
		RPCRT4.dll, apc.dll, d3d.dll,
		CRYPTSP.dll, WES32.dll, NSI.dll,
csrss.exe	380	msvsock.dll, wshtcpip.dll, wship6.dll,
		secur32.dll, SSPICLCL.dll, credssp.dll,
		ADVAPI32.dll,
winlogon.exe	420	ntdll.dll, csrssrv.dll, basesrv.dll,
		win32.dll, USER32.dll, GDI32.dll,
		kernel32.dll, KERNELBASE.dll, LPK.dll,
		USP10.dll, msvcr.dll, sxssrv.dll, sxs.dll,
		RPCRT4.dll, CRYPTBASE.dll,
		RPCRT4.dll, kernel32.dll, LPK.dll, USP10.dll,
		USER32.dll, GDI32.dll, RPCRT4.dll,
		msvcr.dll, WINSTA.dll, RPCRT4.dll,
		IMM32.dll, MSCTF.dll, ADVAPI32.dll,
		sechost.dll, profapi.dll, RPCRT4.dll,
		apc.dll, d3d.dll, CRYPTSP.dll, rsaenh.dll,
		CRYPTBASE.dll, windowscodecs.dll, ole32.dll, wkscl1.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.



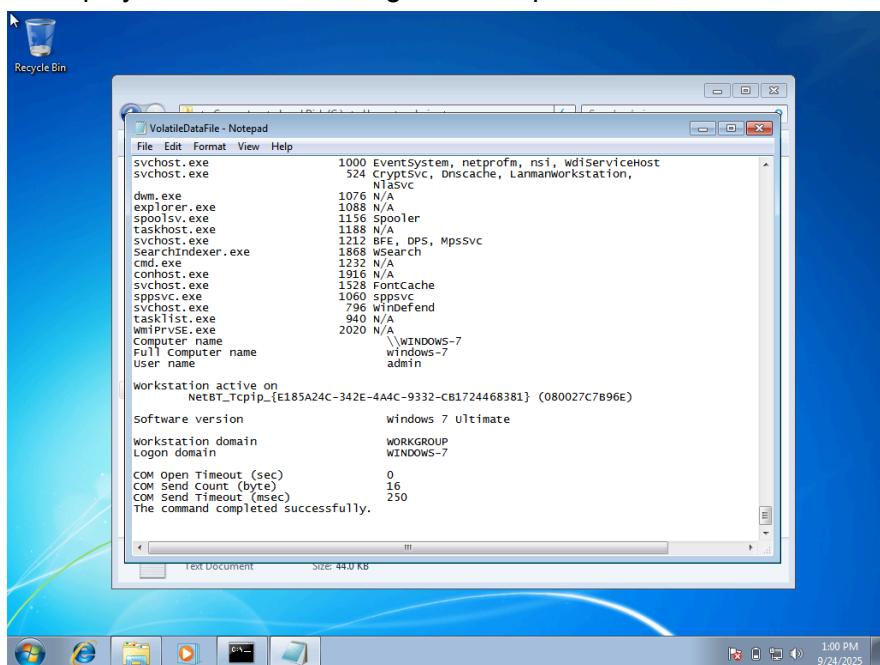
The screenshot shows a Windows desktop environment. In the center is a Notepad window titled "VolatileDataFile - Notepad". The window contains a table with two columns: "Image Name" and "PID Services". The table lists numerous system processes and their corresponding service names. For example, "System Idle Process" has PID 0 and is associated with "N/A". Other entries include "svchost.exe" (PIDs 1000, 524, 1212, 1868, 1916, 1528) which host various services like "EventSystem", "netprof", "nsi", "wdiserviceHost", "CryptSvc", "DnsCache", "LanmanWorkstation", "NtAsvc", "BFE", "DPS", "Mpssvc", "Spooler", "Wsearch", "FontCache", "Sppsvc", "Winefend", "WmiPrvSE", and "TaskList". Other processes listed include "dwm.exe", "explorer.exe", "spoolsv.exe", "taskhost.exe", "svchost.exe", "SearchIndexer.exe", "cmd.exe", "conhost.exe", and "svchost.exe". The Notepad window has a status bar at the bottom indicating "Size: 43.5 KB". The desktop background is blue, and the taskbar at the bottom shows icons for Start, Internet Explorer, File Explorer, and others. The system tray shows the date and time as "9/24/2025 12:57 PM".

Image Name	PID Services
System Idle Process	0 N/A
System	4 N/A
smss.exe	252 N/A
cssrss.exe	320 N/A
wininit.exe	368 N/A
cssrss.exe	384 N/A
winlogon.exe	420 N/A
services.exe	464 N/A
lsass.exe	472 SamSs
lsm.exe	480 N/A
svchost.exe	536 DcomLaunch, PlugPlay, Power
svchost.exe	652 RpcSs
svchost.exe	704 Audiosrv, Dhcp, EventLog, Imhosts, WcsService
svchost.exe	812 AudioEndpointBuilder, CscService, Netman, PcaSVC, SysMain, TrkWks, UxSms, Win32D
svchost.exe	860 AerolookupSVC, AppInfo, Gpsvc, Iphlpsvc, Lammanserver, Profsvc, Schedule, SENS, ShellHWDetection, Themes, Wmigrnt, WuauServ
svchost.exe	1000 EventSystem, NetProf, Nsi, WdiServiceHost, 524 CryptSVC, DnsCache, LanmanWorkstation, NtAsvc
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.



The screenshot shows a Windows desktop environment. In the center is a Notepad window titled "VolatileDataFile - Notepad". The window displays several lines of configuration information. It starts with "workstation active on" followed by a long MAC address. Below that, it shows "Software version" as "windows 7 ultimate". It then lists "workstation domain" as "WORKGROUP" and "Logon domain" as "WINDOWS-7". Under "COM", it shows "Open Timeout (sec)" as 0, "Send Count (byte)" as 16, and "Send Timeout (msec)" as 250. At the bottom, it says "The command completed successfully." The Notepad window has a status bar at the bottom indicating "Size: 44.0 KB". The desktop background is blue, and the taskbar at the bottom shows icons for Start, Internet Explorer, File Explorer, and others. The system tray shows the date and time as "9/24/2025 1:00 PM".

```
workstation active on
    NETBT_Tcpip_{E185A24C-342E-4A4C-9332-CB1724468381} (080027c7896E)

Software version
    windows 7 ultimate

workstation domain
    WORKGROUP

Logon domain
    WINDOWS-7

COM Open Timeout (sec)
    0

COM Send Count (byte)
    16

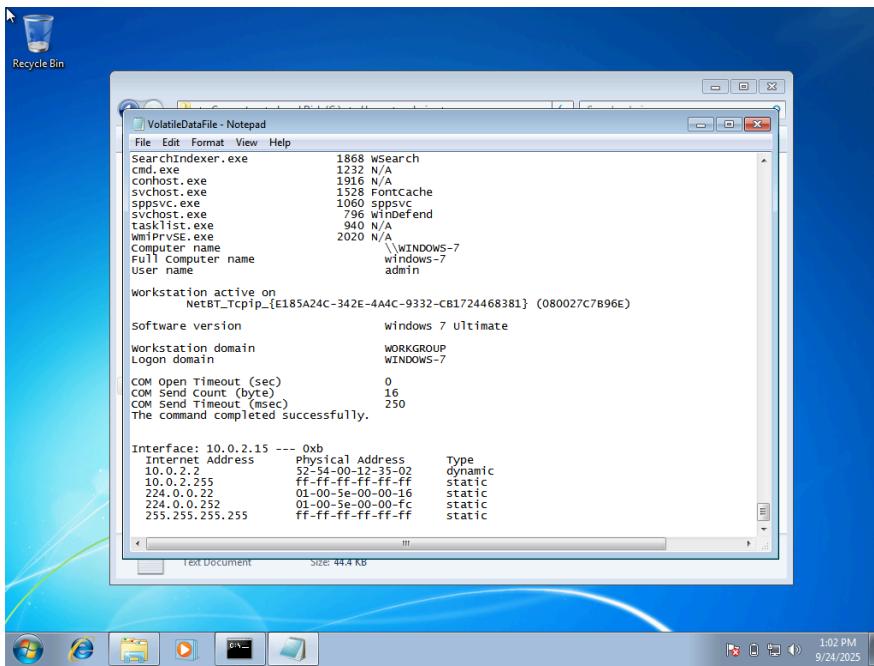
COM Send Timeout (msec)
    250

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.



The screenshot shows a Windows 7 desktop with a Notepad window open. The window title is "VolatileDataFile - Notepad". The content of the Notepad is as follows:

```
Searchchindexer.exe      1868 wsearch
cmd.exe                 1232 N/A
conhost.exe              1916 N/A
svchost.exe              1924 ForCache
spooler.exe               1060 SyncPC
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} (080027c7896E)

Software version          Windows 7 ultimate
Workstation domain        WORKGROUP
Logon domain               WINDOWS-7

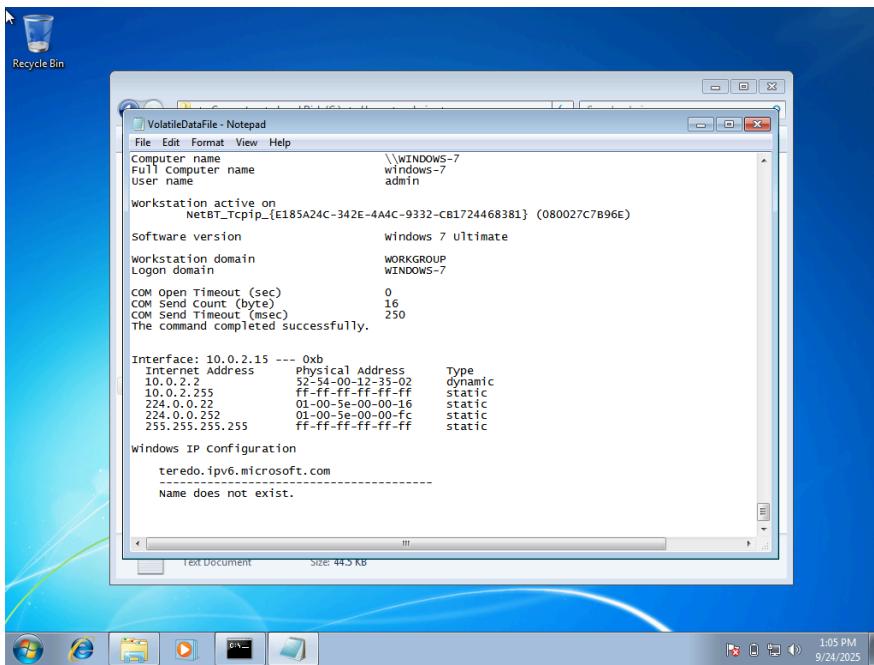
COM Open Timeout (sec)     0
COM Send Count (byte)      16
COM Send Timeout (msec)    250
The command completed successfully.

Interface: 10.0.2.15 --- 0xb
Internet Address          Physical Address      Type
10.0.2.2                  52-54-00-12-3f-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.



The screenshot shows a Windows 7 desktop with a Notepad window open. The window title is "VolatileDataFile - Notepad". The content of the Notepad is as follows:

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

Workstation active on
    NETBT_Tcpip_{E185A24C-342E-4A4C-9332-CB1724468381} (080027c7896E)

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.

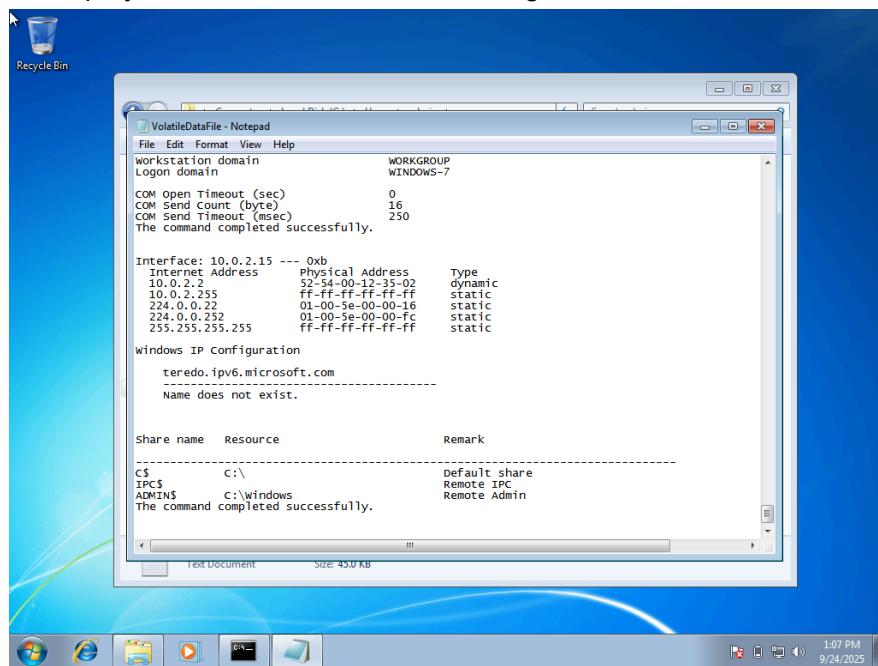
Interface: 10.0.2.15 --- 0xb
Internet Address          Physical Address      Type
10.0.2.2                  52-54-00-12-3f-02  dynamic
10.0.2.255                 ff-ff-ff-ff-ff-ff  static
224.0.0.22                 01-00-5e-00-00-16  static
224.0.0.252                01-00-5e-00-00-fc  static
255.255.255.255           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.



The screenshot shows a Windows desktop environment with a Notepad window open. The window title is "VolatileDataFile - Notepad". The content of the Notepad is as follows:

```
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-00-00-1c  static
255.255.255.255            ff-ff-ff-ff-ff-ff  static

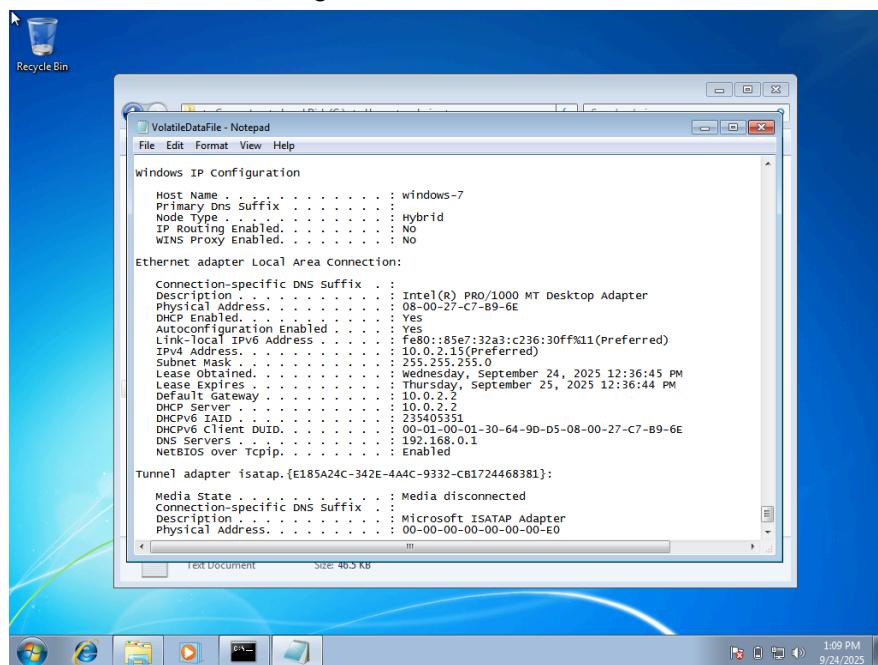
windows IP Configuration
teredo.ipv6.microsoft.com
Name does not exist.

share name   Resource           Remark
-----        -----
C$           C:\                Default share
IPC$          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.



The screenshot shows a Windows desktop environment with a Notepad window open. The window title is "VolatileDataFile - Notepad". The content of the Notepad is as follows:

```
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 . : 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 . . . . . : 00-01-00-01-30-64-90-D5-08-00-27-C7-B9-6E
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{E185A24C-342E-4AAC-9332-C81724468381}:

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

```