Step-by-Step RDP Cache Security Cleanup Guide

Two-Machine Setup: Windows 11 Enterprise + Windows Server 2025

🎯 Our Goal

We'll create a real RDP session from Windows 11 → Windows Server, then:

1. Detect the RDP cache created on Windows 11 (client)
2. Analyze what data is cached
3. Securely delete the cache
4. Verify deletion was successful

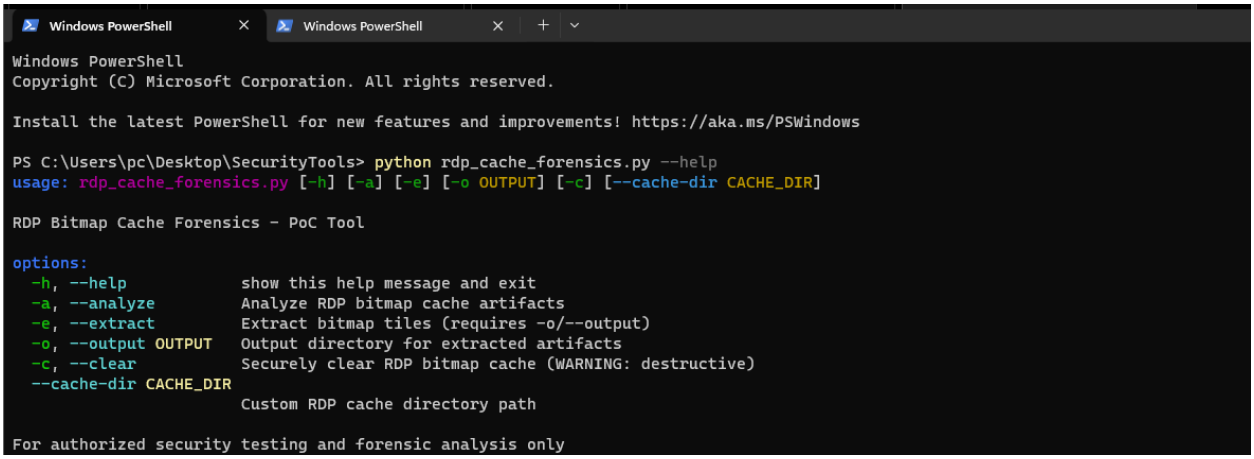
Important: RDP cache is stored on the **CLIENT** machine (Windows 11), not the server!

🎒 Pre-Flight Checklist

On Windows 11 (Client - Where You'll Run the Tool)

```powershell
# 1. Check Python is installed
python --version
# Expected: Python 3.x.x

# 2. Check Pillow is installed
python -c "import PIL; print('Pillow OK')"
# Expected: "Pillow OK"

# 3. Verify tool exists
cd C:\Users\Administrator\Desktop\SecurityTools
dir rdp_cache_forensics.py
# Expected: File should be listed

# 4. Test tool
python rdp_cache_forensics.py --help
# Expected: Help menu displays
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\pc> python --version
Python 3.14.2
PS C:\Users\pc> python -c "import PIL; print('Pillow OK')"
Pillow OK
```



On Windows Server (Remote Target)

powershell

 # 1. Check RDP is enabled

Get-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections"

 # Expected: fDenyTSConnections : 0 (0 = enabled, 1 = disabled)

 # 2. If disabled, enable it:

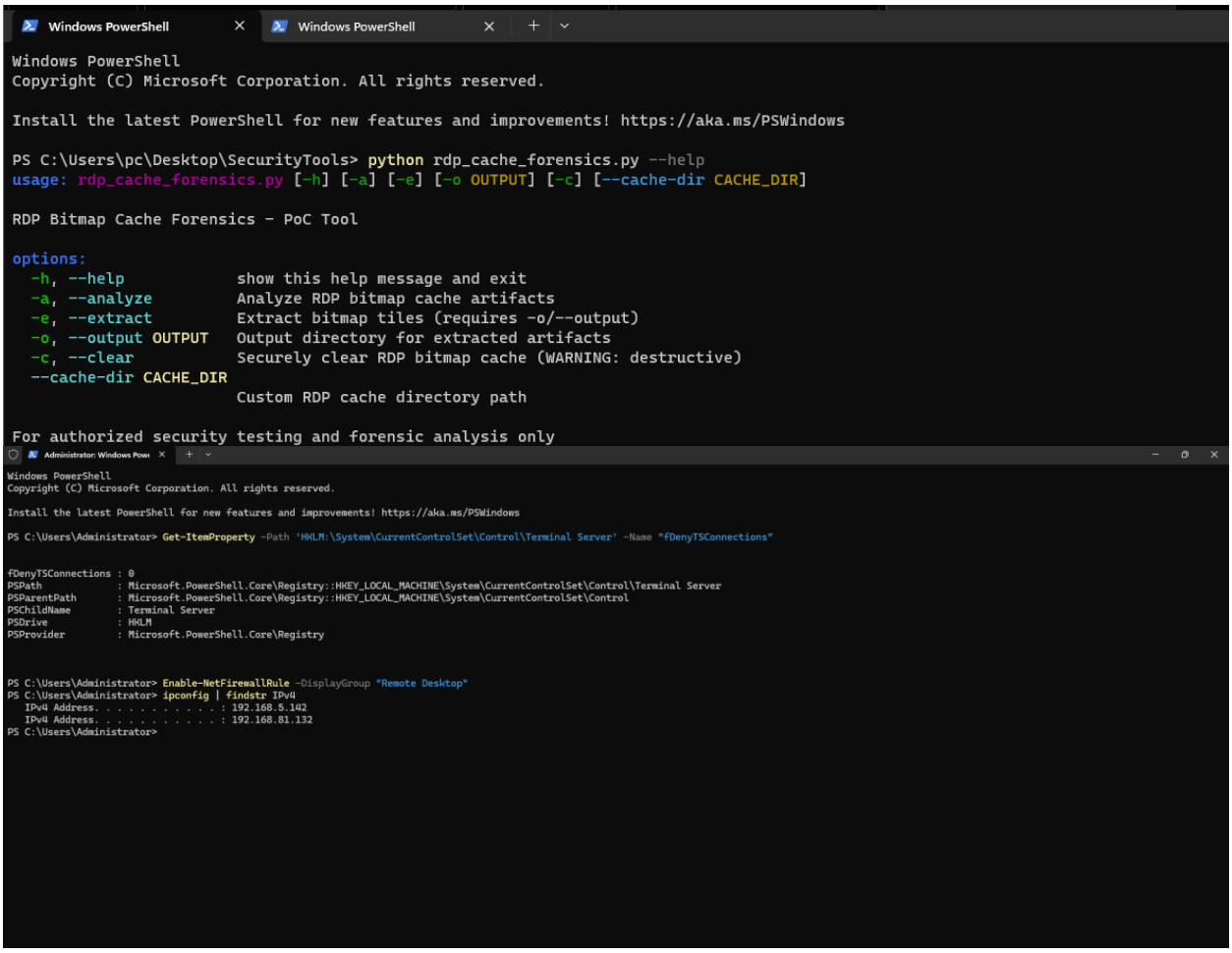
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

 # 3. Get server's IP address

ipconfig | findstr IPv4

 # Note this IP address - you'll need it!



🚀 PHASE 1: Establish Baseline (Windows 11)

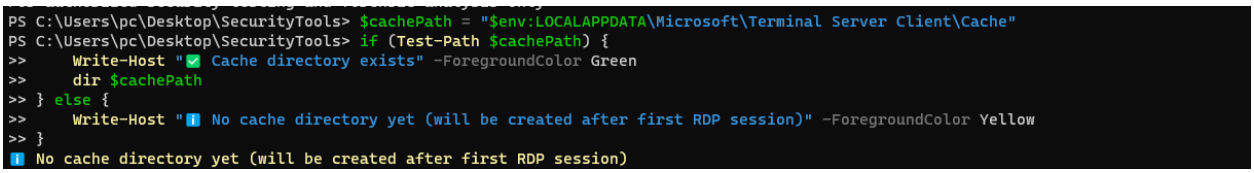
Purpose: Check if any old RDP cache exists before our test

Step 1: Check Current Cache State

On Windows 11, open PowerShell and run:

```
powershell
# Navigate to tool directory
cd C:\Users\Administrator\Desktop\SecurityTools

# Check if cache directory exists
$cachePath = "$env:LOCALAPPDATA\Microsoft\Terminal Server Client\Cache"
if (Test-Path $cachePath) {
    Write-Host "✓ Cache directory exists" -ForegroundColor Green
```

```
    dir $cachePath
} else {
    Write-Host "ℹ No cache directory yet (will be created after first RDP session)" -ForegroundColor Yellow
}
```



Perfect! This confirms you have a clean slate - no RDP cache exists yet on your Windows 11 machine. This is ideal for testing!

Now let's proceed to create an RDP session to generate the cache.

🚀 Next Step: Get Server IP and Connect

Step 1: Get Your Windows Server IP Address

On your Windows Server, open PowerShell and run:

```
powershell
ipconfig | findstr IPv4
```

You should see something like:

```
IPv4 Address. . . . . . . . . . . : 192.168.81.1
```

Write down that IP address!

Step 2: Connect from Windows 11 to Server

Back on your Windows 11 machine (where you just ran the cache check), run:

```
powershell
# Replace YOUR-SERVER-IP with the actual IP from Step 1
mstsc /v:YOUR-SERVER-IP

# For example:
# mstsc /v:192.168.1.100
```

```

**Or use the GUI method:**

1. Press `Windows Key + R`
2. Type: `mstsc`
3. Press Enter
4. Enter the server IP address
5. Click "Connect"

---

### Step 3: Login and Perform Activities

**Once connected to the server:**

1. **Open Notepad** and type sensitive data:
```
SECRET PASSWORD: MyP@ssw0rd2026!
Database Server: 192.168.1.200
Admin User: sa / DbAdmin123
Credit Card: 4532-1234-5678-9000
```

2. **Open File Explorer** and browse:
   - Navigate to `C:\Windows\System32`
   - Browse through some folders
   - Open `C:\Program Files`
3. **Open Command Prompt** and run:

```
cmd
dir C:\
ipconfig
whoami
net user
```

4. **Open Calculator** and do some calculations
5. **WAIT 60 seconds** with all windows visible (let RDP cache the screen)

Step 4: Disconnect (IMPORTANT!)

Critical: You MUST disconnect, not sign out!
```

Correct way:

- Click the **X** button on the RDP window
- When prompted, click **"OK"** or **"Disconnect"**

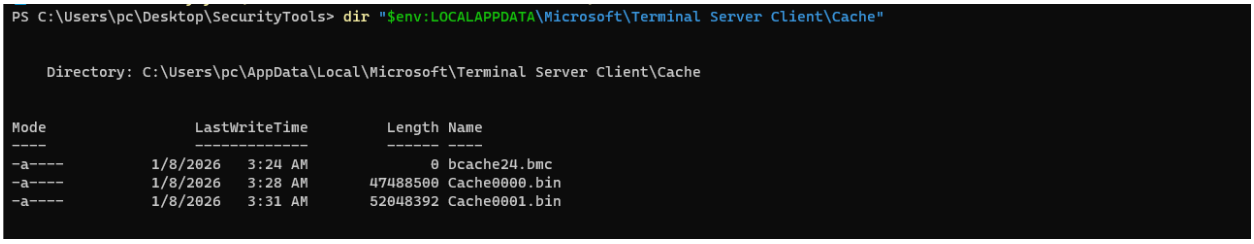
❌ Do NOT:

- Click "Sign out" from Start menu
- Close the session from Task Manager

Expected Results:

Scenario A: Directory exists with files

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/7/2026   3:45 PM        4194304 Cache0000.bin
-a----         1/7/2026   3:45 PM        4194304 Cache0001.bin
```



→ You have old RDP cache from previous sessions

Step 2: Analyze Existing Cache (If Any)

If cache files exist, analyze them:

powershell

```
python rdp_cache_forensics.py --analyze
```

```
PS C:\Users\pc\Desktop\SecurityTools> python rdp_cache_forensics.py --analyze

======================================================================
RDP BITMAP CACHE FORENSIC ANALYSIS
======================================================================

Cache Directory: C:\Users\pc\AppData\Local\Microsoft\Terminal Server Client\Cache
Analysis Time: 2026-01-08T03:31:49.263079
Files Found: 3
Total Size: 99,536,892 bytes (94.93 MB)

----------------------------------------------------------------------
CACHE FILES DISCOVERED:
----------------------------------------------------------------------

[1] bcache24.bmc
    Size: 0 bytes
    Modified: 2026-01-08T03:24:05.496224
    Accessed: 2026-01-08T03:24:05.496224

[2] Cache0000.bin
    Size: 47,488,500 bytes
    Modified: 2026-01-08T03:28:32.117654
    Accessed: 2026-01-08T03:30:02.619303
    Header Signature: 52445038
    Hash: 467181c14de90b1d

[3] Cache0001.bin
    Size: 52,048,392 bytes
    Modified: 2026-01-08T03:31:15.533443
    Accessed: 2026-01-08T03:31:15.533443
    Header Signature: 52445038
    Hash: 467181c14de90b1d

======================================================================
SECURITY IMPLICATIONS:
======================================================================

• These cache files persist after RDP sessions end
• May contain fragments of sensitive information displayed during sessions
• Can be recovered using forensic tools (BMCViewer, custom parsers)
• Accessible by anyone with file system access to the endpoint
• Should be cleared after sensitive RDP sessions
• Consider disabling bitmap caching for high-security environments
```

🗑 PHASE 4: Extract Cache Tiles (Forensic Recovery)

Purpose: Demonstrate what an attacker could recover from these files

Step 1: Create Output Directory

powershell

```
mkdir C:\RDP_Forensics_Evidence
```

Step 2: Extract Bitmap Tiles

powershell

```
python rdp_cache_forensics.py --analyze --extract --output "C:\RDP_Forensics_Evidence"
```

```
PS C:\Users\pc\Desktop\SecurityTools> mkdir RDP_Forensic_Evidence


    Directory: C:\Users\pc\Desktop\SecurityTools


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          1/8/2026   3:36 AM                RDP_Forensic_Evidence


PS C:\Users\pc\Desktop\SecurityTools> python rdp_cache_forensics.py --analyze --extract --output "C:\RDP_Forensics_Evidence"

======================================================================
RDP BITMAP CACHE FORENSIC ANALYSIS
======================================================================

Cache Directory: C:\Users\pc\AppData\Local\Microsoft\Terminal Server Client\Cache
Analysis Time: 2026-01-08T03:36:19.863814
Files Found: 3
Total Size: 99,536,892 bytes (94.93 MB)

----------------------------------------------------------------------
CACHE FILES DISCOVERED:
----------------------------------------------------------------------

[1] bcache24.bmc
    Size: 0 bytes
    Modified: 2026-01-08T03:24:05.496224
    Accessed: 2026-01-08T03:24:05.496224
    Tiles Extracted: 0

[2] Cache0000.bin
    Size: 47,488,500 bytes
    Modified: 2026-01-08T03:28:32.117654
    Accessed: 2026-01-08T03:31:49.292531
    Header Signature: 52445038
    Hash: 467181c14de90b1d

[3] Cache0001.bin
    Size: 52,048,392 bytes
    Modified: 2026-01-08T03:31:15.533443
    Accessed: 2026-01-08T03:31:49.407536
    Header Signature: 52445038
    Hash: 467181c14de90b1d
    Tiles Extracted: 82

======================================================================
SECURITY IMPLICATIONS:
======================================================================

• These cache files persist after RDP sessions end
• May contain fragments of sensitive information displayed during sessions
• Can be recovered using forensic tools (BMCViewer, custom parsers)
• Accessible by anyone with file system access to the endpoint
• Should be cleared after sensitive RDP sessions
• Consider disabling bitmap caching for high-security environments


[✓] Extracted artifacts saved to: C:\RDP_Forensics_Evidence
PS C:\Users\pc\Desktop\SecurityTools> python rdp_cache_forensics.py --clear

[!] WARNING: This will permanently delete cache files. Continue? (yes/no): yes

======================================================================
RDP BITMAP CACHE SECURE CLEARING
======================================================================

Files Processed: 3
Files Deleted: 3
Total Bytes Cleared: 99,536,892 bytes
```

Step 3: Examine Extracted Files

```
powershell
# View extracted files
dir C:\RDP_Forensics_Evidence
# Count how many tiles were extracted
(Get-ChildItem C:\RDP_Forensics_Evidence).Count
```

What you'll see:

```
Cache0000_tile_0001.bin
Cache0000_tile_0002.bin
Cache0000_tile_0003.bin
...
Cache0001_tile_0001.bin
...
```

```
PS C:\Users\pc\Desktop\SecurityTools> dir C:\RDP_Forensics_Evidence


    Directory: C:\RDP_Forensics_Evidence


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0000.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0001.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0002.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0003.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0004.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0005.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0006.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0007.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0008.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0009.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0010.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0011.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0012.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0013.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0014.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0015.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0016.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0017.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0018.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0019.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0020.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0021.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0022.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0023.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0024.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0025.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0026.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0027.bin
-a----          1/8/2026   3:36 AM          65536 Cache0000_tile_0028.bin
```

Note: These are raw bitmap fragments. Professional forensic tools like **BMCViewer** can reconstruct these into viewable images showing:

- Your Notepad with "SECRET PASSWORD"

- Command Prompt outputs
- File Explorer windows
- Everything visible during the session!

🔥 PHASE 5: Secure Cache Deletion

Purpose: Permanently and securely remove RDP cache

Step 1: Understand What Will Happen

⚠ WARNING:

- This will **permanently delete** all RDP cache files
- Files will be overwritten 3 times before deletion
- Cannot be recovered after deletion
- Affects **all** cached RDP sessions, not just the recent one

Step 2: Run Secure Clearing

powershell

```
python rdp_cache_forensics.py --clear
```

You'll see this prompt:

```
[!] WARNING: This will permanently delete cache files. Continue? (yes/no):
```

Type: `yes` (then press Enter)

Expected output:

```
PS C:\Users\pc\Desktop\SecurityTools> python rdp_cache_forensics.py --clear

[!] WARNING: This will permanently delete cache files. Continue? (yes/no): yes

======================================================================
RDP BITMAP CACHE SECURE CLEARING
======================================================================

Files Processed: 3
Files Deleted: 3
Total Bytes Cleared: 99,536,892 bytes

[✓] All cache files successfully cleared
PS C:\Users\pc\Desktop\SecurityTools>
                                    python rdp_cache_forensics.py --analyze

======================================================================
RDP BITMAP CACHE FORENSIC ANALYSIS
======================================================================

Cache Directory: C:\Users\pc\AppData\Local\Microsoft\Terminal Server Client\Cache
Analysis Time: 2026-01-08T08:44:45.461241
Files Found: 0
Total Size: 0 bytes (0.00 MB)

======================================================================
SECURITY IMPLICATIONS:
======================================================================

• These cache files persist after RDP sessions end
• May contain fragments of sensitive information displayed during sessions
• Can be recovered using forensic tools (BMCViewer, custom parsers)
• Accessible by anyone with file system access to the endpoint
• Should be cleared after sensitive RDP sessions
• Consider disabling bitmap caching for high-security environments
```

Step 3: Verify Deletion

powershell

 # Check if cache directory is empty

dir "$env:LOCALAPPDATA\Microsoft\Terminal Server Client\Cache"

✅ Success:

```
PS C:\Users\pc\Desktop\SecurityTools>
                                    > dir "$env:LOCALAPPDATA\Microsoft\Terminal Server Client\Cache"
PS C:\Users\pc\Desktop\SecurityTools>
```

Step 4: Confirm with Tool

powershell

python rdp_cache_forensics.py --analyze

Expected output:

```
PS C:\Users\pc\Desktop\SecurityTools> python rdp_cache_forensics.py --analyze

======================================================================
RDP BITMAP CACHE FORENSIC ANALYSIS
======================================================================

Cache Directory: C:\Users\pc\AppData\Local\Microsoft\Terminal Server Client\Cache
Analysis Time: 2026-01-08T10:14:54.911373
Files Found: 0
Total Size: 0 bytes (0.00 MB)

======================================================================
SECURITY IMPLICATIONS:
======================================================================

• These cache files persist after RDP sessions end
• May contain fragments of sensitive information displayed during sessions
• Can be recovered using forensic tools (BMCViewer, custom parsers)
• Accessible by anyone with file system access to the endpoint
• Should be cleared after sensitive RDP sessions
• Consider disabling bitmap caching for high-security environments

PS C:\Users\pc\Desktop\SecurityTools>
```

🛡 PHASE 8: Implement Ongoing Protection

Option 1: Manual Clearing (Quick Fix)

Create desktop shortcut for quick cache clearing:

```powershell
# Create shortcut on desktop
$WshShell = New-Object -ComObject WScript.Shell
$Shortcut = $WshShell.CreateShortcut("$env:USERPROFILE\Desktop\Clear RDP Cache.lnk")
$Shortcut.TargetPath = "powershell.exe"
$Shortcut.Arguments = "-ExecutionPolicy Bypass -Command `"cd 'C:\Users\Administrator\Desktop\SecurityTools'; python rdp_cache_forensics.py --clear`""
$Shortcut.IconLocation = "shell32.dll,131"
$Shortcut.Description = "Securely clear RDP bitmap cache"
$Shortcut.Save()

Write-Host "✅ Desktop shortcut created: 'Clear RDP Cache'" -ForegroundColor Green
```

Usage: Double-click the shortcut after any RDP session

Option 2: Automated Clearing Script

Create logoff script:

```powershell
# Create script directory
mkdir C:\Scripts -ErrorAction SilentlyContinue

# Create clearing script
@'
# Auto-Clear-RDP-Cache.ps1
$cachePath = "$env:LOCALAPPDATA\Microsoft\Terminal Server Client\Cache"

if (Test-Path $cachePath) {
    try {
        # Overwrite and delete
        Get-ChildItem $cachePath -File | ForEach-Object {
            $zeros = New-Object byte[] $_.Length
            [System.IO.File]::WriteAllBytes($_.FullName, $zeros)
        }
        Remove-Item "$cachePath\*" -Force -ErrorAction SilentlyContinue

        # Log success
        Add-Content "C:\Scripts\rdp-cache-clear.log" "$(Get-Date) - Cache cleared successfully"
    }
    catch {
        Add-Content "C:\Scripts\rdp-cache-clear.log" "$(Get-Date) - ERROR: $_"
    }
}
'@ | Out-File C:\Scripts\Auto-Clear-RDP-Cache.ps1

Write-Host "✅ Script created: C:\Scripts\Auto-Clear-RDP-Cache.ps1" -ForegroundColor Green
```

Schedule it to run at logoff:

```powershell
# Create scheduled task
$action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-ExecutionPolicy Bypass -File C:\Scripts\Auto-Clear-RDP-Cache.ps1"
$trigger = New-ScheduledTaskTrigger -AtLogOff
```

```
$principal = New-ScheduledTaskPrincipal -UserId "$env:USERNAME" -RunLevel Highest
$settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries

Register-ScheduledTask -TaskName "Clear RDP Cache at Logoff" -Action $action -Trigger $trigger -Principal $principal -Settings $settings -Description "Automatically clears RDP bitmap cache at user logoff"

Write-Host "✅ Scheduled task created: Will run at every logoff" -ForegroundColor Green
```

Option 3: Disable Bitmap Caching (Most Secure)

⚠ Warning: May reduce RDP performance

```
powershell
# Disable persistent bitmap caching
Set-ItemProperty -Path "HKCU:\Software\Microsoft\Terminal Server Client" -Name "BitmapPersistCacheSize" -Value 0 -Type DWord

Write-Host "✅ Bitmap caching disabled" -ForegroundColor Green
Write-Host "ℹ Note: RDP performance may be slightly reduced" -ForegroundColor Yellow
```

To re-enable if needed:

```
powershell
Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Terminal Server Client" -Name "BitmapPersistCacheSize"
```