```
# ==============================================
# DNS FORENSIC COMPANION - ENFORCER
# ==============================================

$ErrorActionPreference = 'Stop'

$BasePath = 'C:\Users\herbe\OneDrive\Apps\PowerShell\creating_doh_VFINAL\companion_tool'
$LogFile  = Join-Path $BasePath 'dns_forensic_companion.log'
$Rollback = Join-Path $BasePath 'dns_forensic_companion.rollback.json'

$AllowedDNS = @(
    '1.1.1.1','1.0.0.1',
    '2606:4700:4700::1111','2606:4700:4700::1001'
)

if (-not (Test-Path $BasePath)) {
    New-Item -ItemType Directory -Path $BasePath -Force | Out-Null
}

function Log {
    param([string]$Message)
    $line = "[{0}] {1}" -f (Get-Date -Format 'yyyy-MM-dd HH:mm:ss'), $Message
    Add-Content -Path $LogFile -Value $line
}

Log '=== COMPANION ENFORCER START ==='

# ----------------------------
# SNAPSHOT FOR ROLLBACK
# ----------------------------
$Snapshot = @{
    Timestamp = (Get-Date).ToString('o')
    Adapters  = @()
    Registry  = @()
}

# ----------------------------
# ADAPTER DNS ENFORCEMENT
# ----------------------------
Get-DnsClient |
Where-Object { $_.ConnectionState -eq 'Connected' } |
ForEach-Object {

    $addresses = Get-DnsClientServerAddress `
        -InterfaceIndex $_.InterfaceIndex `
        -AddressFamily IPv4,IPv6

    $dns = $addresses.ServerAddresses

    $Snapshot.Adapters += @{
        Interface = $_.InterfaceAlias
        DNS       = $dns
    }

    if ($dns | Where-Object { $_ -notin $AllowedDNS }) {
        Log "DRIFT adapter [$($_.InterfaceAlias)] — correcting"
        Set-DnsClientServerAddress `
            -InterfaceIndex $_.InterfaceIndex `
            -ServerAddresses $AllowedDNS
    }
}

# ----------------------------
# REGISTRY TCP/IP CLEANUP
# ----------------------------
$regRoots = @(
    'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters',
    'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces'
)

foreach ($root in $regRoots) {
    Get-ChildItem $root -ErrorAction SilentlyContinue | ForEach-Object {
```

```powershell

        foreach ($field in 'NameServer','DhcpNameServer') {

            $value = (Get-ItemProperty $_.PsPath -Name $field -ErrorAction SilentlyContinue).$field
            if (-not $value) { continue }

            $dns = ($value -split '[ ,]+' | Where-Object { $_ -ne '' })

            if ($dns | Where-Object { $_ -notin $AllowedDNS }) {

                $Snapshot.Registry += @{
                    Path  = $_.PsPath
                    Field = $field
                    Value = $value
                }

                Log "DRIFT registry [$($_.PSChildName)] $field – cleared"
                Remove-ItemProperty -Path $_.PsPath -Name $field -ErrorAction SilentlyContinue
            }
        }
    }
}

# ----------------------------
# SAVE ROLLBACK
# ----------------------------
$Snapshot | ConvertTo-Json -Depth 6 |
Set-Content -Path $Rollback -Encoding UTF8

Log '=== COMPANION ENFORCER END ==='
exit 10

```