PROJECT

[Hashing Algorithms + Coding up a File Integrity Monitor (FIM)]

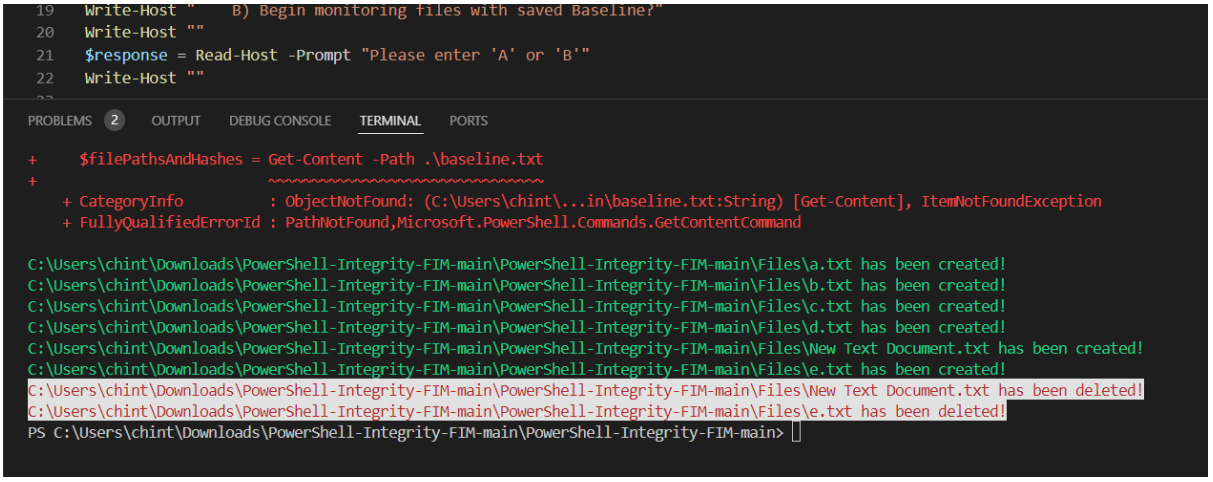
Code:

```
Function Calculate-File-Hash($filepath) {
    $filehash = Get-FileHash -Path $filepath -Algorithm SHA512
    return $filehash
}

Function Erase-Baseline-If-Already-Exists() {
    $baselineExists = Test-Path -Path .\baseline.txt

    if ($baselineExists) {
        # Delete it
        Remove-Item -Path .\baseline.txt
    }
}

Write-Host ""
Write-Host "What would you like to do?"
Write-Host ""
Write-Host "    A) Collect new Baseline?"
Write-Host "    B) Begin monitoring files with saved Baseline?"
Write-Host ""
$response = Read-Host -Prompt "Please enter 'A' or 'B'"
Write-Host ""

if ($response -eq "A".ToUpper()) {
    # Delete baseline.txt if it already exists
    Erase-Baseline-If-Already-Exists

    # Calculate Hash from the target files and store in baseline.txt
    # Collect all files in the target folder
    $files = Get-ChildItem -Path .\Files -Recurse

    # For each file, calculate the hash, and write to baseline.txt
    foreach ($f in $files) {
        $hash = Calculate-File-Hash $f.FullName
        "$($hash.Path)|$($hash.Hash)" | Out-File -FilePath
.\baseline.txt -Append
```

```
    }
}

elseif ($response -eq "B".ToUpper()) {
    $fileHashDictionary = @{}

    # Load file|hash from baseline.txt and store them in a dictionary
    $filePathsAndHashes = Get-Content -Path .\baseline.txt

    foreach ($f in $filePathsAndHashes) {
        $fileHashDictionary.Add($f.Split("|")[0],$f.Split("|")[1])
    }

    # Begin (continuously) monitoring files with saved Baseline
    while ($true) {
        Start-Sleep -Seconds 1

        $currentFiles = Get-ChildItem -Path .\Files -Recurse

        # Check for new files or changes in existing files
        foreach ($file in $currentFiles) {
            $hash = Calculate-File-Hash $file.FullName
            if (-not $fileHashDictionary.ContainsKey($hash.Path)) {
                # A new file has been created!
                Write-Host "$($hash.Path) has been created!"
-ForegroundColor Green
                $fileHashDictionary[$hash.Path] = $hash.Hash
            }
            elseif ($fileHashDictionary[$hash.Path] -ne $hash.Hash) {
                # The file has changed
                Write-Host "$($hash.Path) has changed!!!"
-ForegroundColor Yellow
                $fileHashDictionary[$hash.Path] = $hash.Hash
            }
        }
# Check for deleted files
foreach ($key in $fileHashDictionary.Keys) {
    if (-not (Test-Path -Path $key)) {
        # The file has been deleted
        Write-Host "$($key) has been deleted!" -ForegroundColor DarkRed
-BackgroundColor Gray
        $fileHashDictionary.Remove($key)
    }
```

```
}


    }
}
```

Output :



[As seen in output that it shoes created and new created file alert at initial stage and then if new .txt file is created it also generates alert for that and if any file is deleted that alert kind of alert also generated]

Thank You !