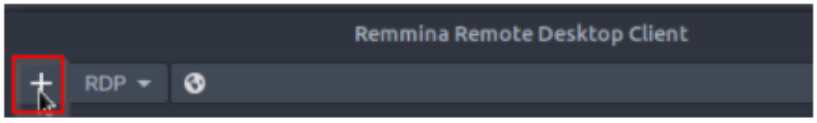
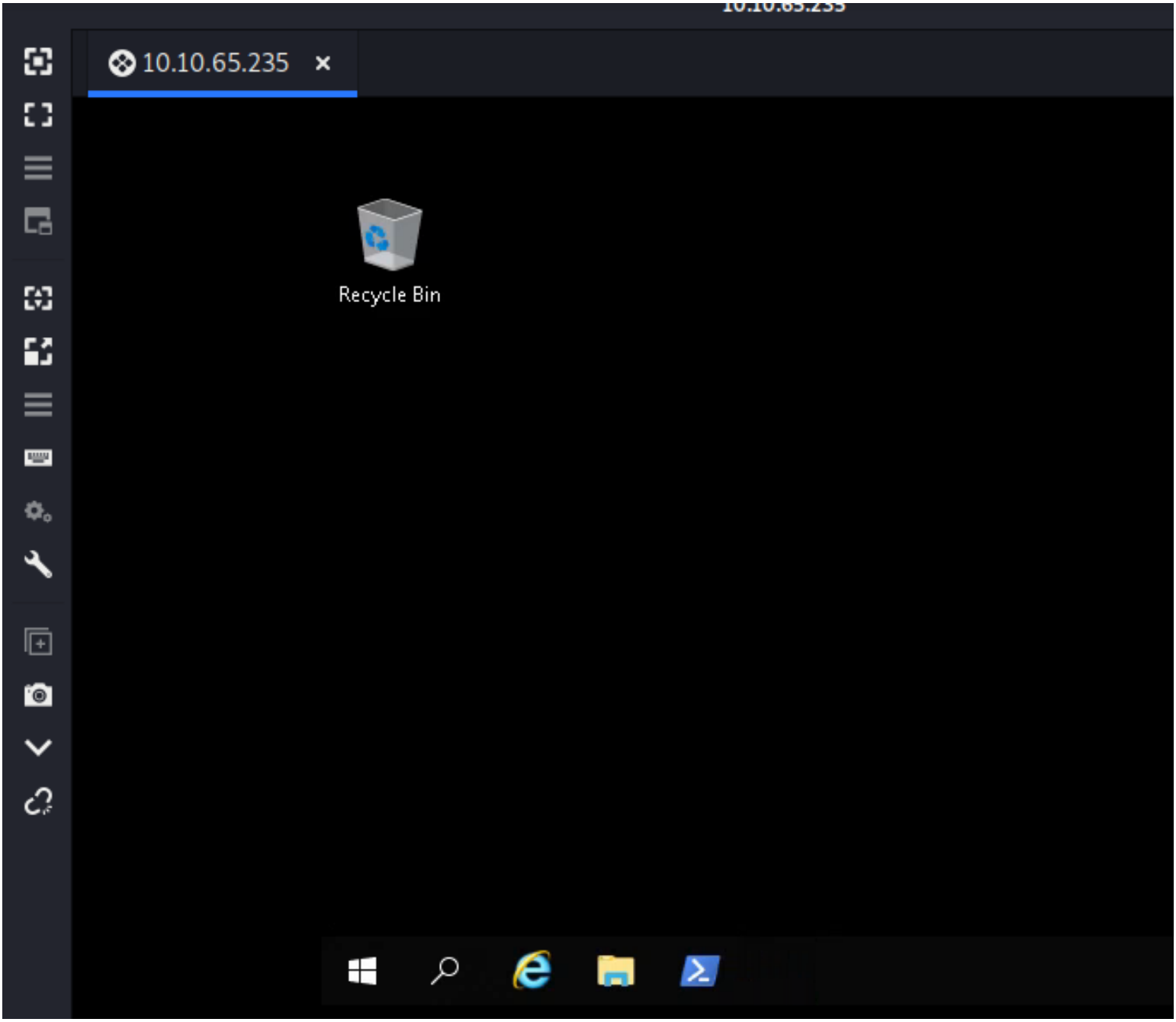
Day 21 - Time for some ELForensics

Scenario

> One of the 'little helpers' logged into his workstation only to realize that the database connector file has been replaced, and he can't find th naughty list anymore. Furthermore, upon executing the database connector file, a taunting message was displayed, hinting that the file was moved to another location.
>
> McEager has been notified, and he will put the pieces together to find the database connector file.
>
> Watch DarkStar's Video On Solving The Task Here.
>
> **Task**: Find where the database connector file is hidden using forensic-like investigative techniques.
>
> ---
>
> You can use the **AttackBox** and **Remmina** to connect to the remote machine. Make sure the remote machine is deployed before proceeding.
>
> Click on the plus icon as shown below.
>
> 
>
>
> For **Server** provide (`10.10.219.166`) as the IP address provided to you for the remote machine. The credentials for the user account is:
>
> - User name: `littlehelper`
> - User password: `iLoveSnow!`

access the RDP port of the remote host using remmina



now go to document directory & there's 2 files

```
PS C:\Users\littlehelper\Documents> get-childitem


    Directory: C:\Users\littlehelper\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/23/2020  11:21 AM             63 db file hash.txt
-a----        11/23/2020  11:22 AM           5632 deebee.exe
```

& that's the hash for db.exe

```
PS C:\Users\littlehelper\Documents> get-content '.\db file hash.txt'
Filename:       db.exe
MD5 Hash:       596690FFC54AB6101932856E6A78E3A1
PS C:\Users\littlehelper\Documents>
```

getting the md5 hash for the mysterious deebee.exe

```
PS C:\Users\littlehelper\Documents> get-filehash -algorithm md5 .\deebee.exe

Algorithm       Hash
---------       ----
MD5             5F037501FB542AD2D9B06EB12AED09F0
```

using strings to find the flag in the mysterious executable

```
args
Object
Accessing the Best Festival Company Database..
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Con
Documents\db.exe).Path -ReadCount 0 -Encoding
```

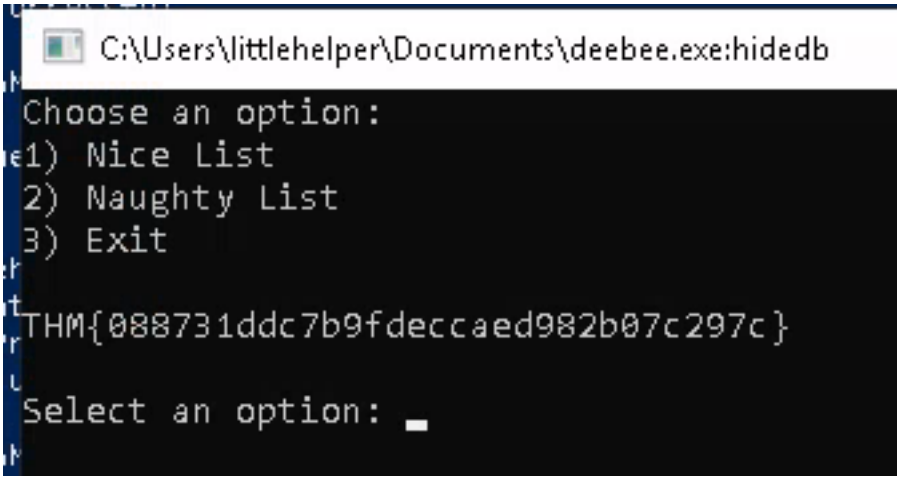
list out all of the Alternate Data Stream (ADS) from the deebee.exe & found the Stream (hidedb) seems kinda sus

```
PS C:\Users\littlehelper\Documents> get-item -path .\deebee.exe -stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\
                deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\
                deebee.exe:hidedb
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe:hidedb
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : hidedb
Length        : 6144
```

use wmic to create a process call of the deebee.exe:hidedb

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-path C:\Users\li
ttlehelper\Documents\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2212;
        ReturnValue = 0;
};

PS C:\Users\littlehelper\Documents>
```

& we found the flag!


C:\Users\littlehelper\Documents\deebee.exe:hidedb
Choose an option:
1) Nice List
2) Naughty List
3) Exit
THM{088731ddc7b9fdeccaed982b07c297c}
Select an option: