

Operációs rendszerek BSc

2. Gyak.

2022. 02. 16.

Készítette:

Vigh Bence Imre Bsc

Programtervező Informatik Szak

E0EOAN

Miskolc, 2022

1.

a.) Hozza létre a következő mappa szerkezetet!

neptunkod

- bokor
 - banan
 - mogyoro
 - barack
- fa
 - korte
- land
 - szeder
 - kokusz

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ mkdir bokor

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ mkdir fa

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ mkdir land

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ cd bokor

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor
$ mkdir banan

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor
$ mkdir mogyoro

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor
$ mkdir barack

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor
$ cd -
/c/Users/user/Desktop/E0EOAN0sGyak/E0EOAN_0216

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ cd fa

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa
$ mkdir korte

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa
$ cd -
/c/Users/user/Desktop/E0EOAN0sGyak/E0EOAN_0216

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ cd land

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/land
$ mkdir szeder

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/land
$ mkdir kokusz

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/land
```

b.) Készítsen másolatot:

a neptunkod/land/szeder katalógusról a neptunkod/fa katalógusba
a neptunkod/bokor/banan katalógusról a neptunkod/fa katalógusba

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ cp -r ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/land/szeder ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa/

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ cp -r ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor/banan ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa/
```

c.) Végezze el a következő áthelyezéseket:

a neptunkod/bokor/barack katalógust helyezze át a neptunkod/fa katalógusba
a neptunkod/land/kokusz katalógust helyezze át a neptunkod/fa katalógusba

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ mv ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/bokor/barack ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa/

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0EOAN0sGyak/E0EOAN_0216
$ mv ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/land/kokusz ~/Desktop/E0EOAN0sGyak/E0EOAN_0216/fa/
```

d.) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

neptunkod/bokor/banan/ leiras.txt

neptunkod/tree/felsorolas.txt

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216
$ rmdir ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/land/szeder

user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216
$ rmdir ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/land
```

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/bokor/banan
$ cat > leiras.txt
```

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/fa
$ cat > felsorolas.txt
```

e.) A leiras.txt szöveges állományba írjon 3 sort a barackról.

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/bokor/banan
$ echo -e "A barack szép \nA barack édes \nA barack jó"
A barack szép
A barack édes
A barack jó
```

```
user@DESKTOP-KCGCMT0 MINGW64 ~/Desktop/E0E0AN0sGyak/E0E0AN_0216/fa
$ echo -e "Máté \nZoltán \nBóldizsár \nMárk \nPéter" > felsorolas.txt
```

f.) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

Cmd re kellett váltanom mivel a "tree" utasítás csak így futott le

```
C:\Users\user>TREE C:\Users\user\Desktop\E0E0AN0sGyak\E0E0AN_0216
Folder PATH listing for volume Boot
Volume serial number is 0000000C 5A37:7636
C:\USERS\USER\DESKTOP\E0E0AN0SGYAK\E0E0AN_0216
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
```

g.) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje e.

```
C:\Users\user\Desktop\E0E0AN0sGyak\E0E0AN_0216>dir /s "?e*"
Volume in drive C is Boot
Volume Serial Number is 5A37-7636

Directory of C:\Users\user\Desktop\E0E0AN0sGyak\E0E0AN_0216\bokor\banan

2022. 02. 21. 12:54                0 leiras.txt
1 File(s)                        0 bytes

Directory of C:\Users\user\Desktop\E0E0AN0sGyak\E0E0AN_0216\fa

2022. 02. 21. 12:47                0 felsorolas.txt
1 File(s)                        0 bytes

Total Files Listed:
2 File(s)                        0 bytes
0 Dir(s) 61 273 853 952 bytes free
```

h.) Tegye mindenki számára olvashatóvá a felsorolas.txt file-t

```
C:\Windows\System32>icacls C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\fa\felsorolas.txt /grant Mindenki:r
processed file: C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\fa\felsorolas.txt
Successfully processed 1 files; Failed processing 0 files
```

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival együtt.

```
C:\Windows\System32>dir /s C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216
Volume in drive C is Boot
Volume Serial Number is 5A37-7636

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216

2022. 02. 21. 12:32 <DIR>      .
2022. 02. 21. 12:32 <DIR>      ..
2022. 02. 21. 12:17 <DIR>      bokor
2022. 02. 21. 12:47 <DIR>      fa
                0 File(s)          0 bytes

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\bokor

2022. 02. 21. 12:17 <DIR>      .
2022. 02. 21. 12:17 <DIR>      ..
2022. 02. 21. 12:42 <DIR>      banan
2022. 02. 21. 10:07 <DIR>      mogyoro
                0 File(s)          0 bytes

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\bokor\banan

2022. 02. 21. 12:42 <DIR>      .
2022. 02. 21. 12:42 <DIR>      ..
2022. 02. 21. 12:54          0 leiras.txt
                1 File(s)          0 bytes

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\bokor\mogyoro

2022. 02. 21. 10:07 <DIR>      .
2022. 02. 21. 10:07 <DIR>      ..
                0 File(s)          0 bytes

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\fa

2022. 02. 21. 12:47 <DIR>      .
2022. 02. 21. 12:47 <DIR>      ..
2022. 02. 21. 10:30 <DIR>      banan
2022. 02. 21. 10:07 <DIR>      barack
2022. 02. 21. 12:47          0 felsorolas.txt
2022. 02. 21. 10:09 <DIR>      kokusz
2022. 02. 21. 10:09 <DIR>      korte
2022. 02. 21. 10:28 <DIR>      szeder
                1 File(s)          0 bytes

Directory of C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\fa\banan

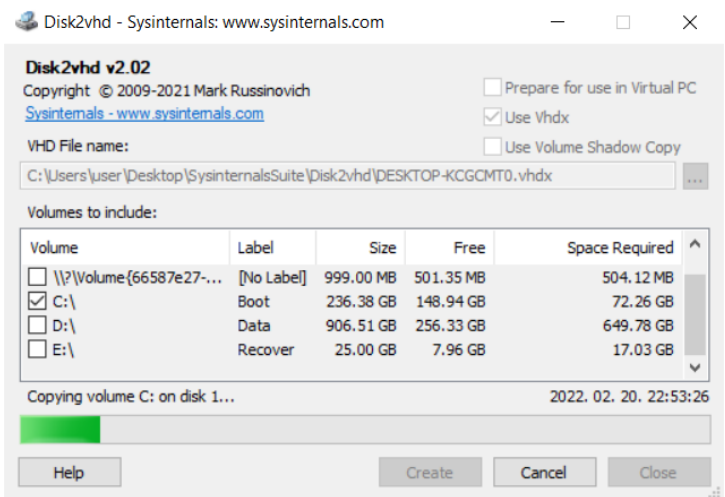
2022. 02. 21. 10:30 <DIR>      .
2022. 02. 21. 10:29 <DIR>      ..
```

j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
C:\Windows\System32>sort C:\Users\user\Desktop\E0EOAN0sGyak\E0EOAN_0216\fa\felsorolas.txt
Boldizsar
Mark
Mate
Peter
Zoltan
```

2. Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.

a.) Disk2vhd



Merevlemez másolást szolgáltat.

b.) TCPView

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1240	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.20.2:11:41	RpcSs
System	4	TCP	Listen	192.168.1.104	139	0.0.0.0	0	2022.02.20.19:13:53	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.20.19:13:53	System
OriginWebHelperServ...	4216	TCP	Listen	127.0.0.1	3213	0.0.0.0	0	2022.02.20.10:20:43	Origin Web Hel...
svchost.exe	7136	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.19:13:50	CDPSvc
Discord.exe	3580	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	2022.02.20.19:14:18	Discord.exe
GCUBridge.exe	4964	TCP	Listen	0.0.0.0	13688	0.0.0.0	0	2022.02.20.2:11:52	GCUBridge
steam.exe	12596	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	2022.02.20.19:14:50	steam.exe
steam.exe	12596	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	2022.02.20.19:14:37	steam.exe
lsass.exe	800	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.20.2:11:41	lsass.exe
wininit.exe	1000	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.20.2:11:41	wininit.exe
svchost.exe	1788	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.20.2:11:42	EventLog
svchost.exe	1620	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.20.2:11:42	Schedule
spoolsv.exe	4488	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.20.2:11:47	Spooler
services.exe	788	TCP	Listen	0.0.0.0	49672	0.0.0.0	0	2022.02.20.2:12:00	services.exe
nvcontainer.exe	4992	TCP	Established	127.0.0.1	52032	127.0.0.1	65001	2022.02.20.19:13:51	nvcontainer.exe
svchost.exe	4580	TCP	Established	192.168.1.104	52110	20.199.120.151	443	2022.02.20.19:13:55	WpnService
NVIDIA Web Helper.exe	1188	TCP	Listen	127.0.0.1	52146	0.0.0.0	0	2022.02.20.19:14:02	NVIDIA Web Hel...
chrome.exe	5784	TCP	Established	192.168.1.104	54804	142.250.27.188	5228	2022.02.20.20:15:52	chrome.exe
Video.UI.exe	14900	TCP	Established	192.168.1.104	55284	23.47.212.11	443	2022.02.20.19:15:03	Video.UI.exe
Video.UI.exe	14900	TCP	Established	192.168.1.104	55285	104.18.25.243	80	2022.02.20.19:15:03	Video.UI.exe
Discord.exe	2228	TCP	Established	192.168.1.104	58643	162.159.130.234	443	2022.02.20.22:56:23	Discord.exe
Bliss.exe	14080	TCP	Close Wait	192.168.1.104	61008	104.10.128.76	443	2022.02.20.22:56:15	Bliss.exe

Endpoints: 101 Established: 11 Listening: 32 Time Wait: 1 Close Wait: 4 Update: 2 sec States: (All)

Hálózati megfigyelés/adatforgalom.

c.) Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-KCGCMT0\user]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 028 K	34 816 K	124		
System Idle Process	86.65	60 K	8 K	0		
System	0.75	200 K	3 916 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 076 K	1 044 K	764		
Memory Compression		912 K	341 848 K	2920		
csrss.exe		1 996 K	5 932 K	860		
wininit.exe		1 736 K	6 860 K	1000		
services.exe	1.32	6 084 K	9 832 K	788		
svchost.exe		13 460 K	33 616 K	1056	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		3 652 K	10 560 K	3596		
SettingSyncHost.exe		4 324 K	7 180 K	4004	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperienceHo...		34 904 K	89 928 K	10288		
RuntimeBroker.exe		5 984 K	24 084 K	2680	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	118 460 K	203 404 K	10228	Search application	Microsoft Corporation
RuntimeBroker.exe		12 744 K	38 816 K	3164	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	33 720 K	31 624 K	10988		Microsoft Corporation
LockApp.exe	Susp...	15 700 K	53 048 K	13076	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10 128 K	32 596 K	9912	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	< 0.01	6 520 K	24 404 K	8212	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 428 K	20 684 K	10560	Runtime Broker	Microsoft Corporation
TextInputHost.exe		14 132 K	49 540 K	1884		Microsoft Corporation
ShellExperienceHost.exe	Susp...	24 752 K	82 508 K	9864	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		6 204 K	25 608 K	2516	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.e...		9 780 K	28 164 K	14352	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	28 656 K	2 708 K	9404	Gépház	Microsoft Corporation
UserOOBEBroker.exe		2 012 K	9 464 K	15760	User OOBEBroker	Microsoft Corporation
Video.UI.exe	Susp...	21 076 K	3 120 K	14900		
RuntimeBroker.exe		1 604 K	7 428 K	14072	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	364 656 K	419 504 K	15404	Search application	Microsoft Corporation

CPU Usage: 14.32% Commit Charge: 49.16% Processes: 205 Physical Usage: 38.64%

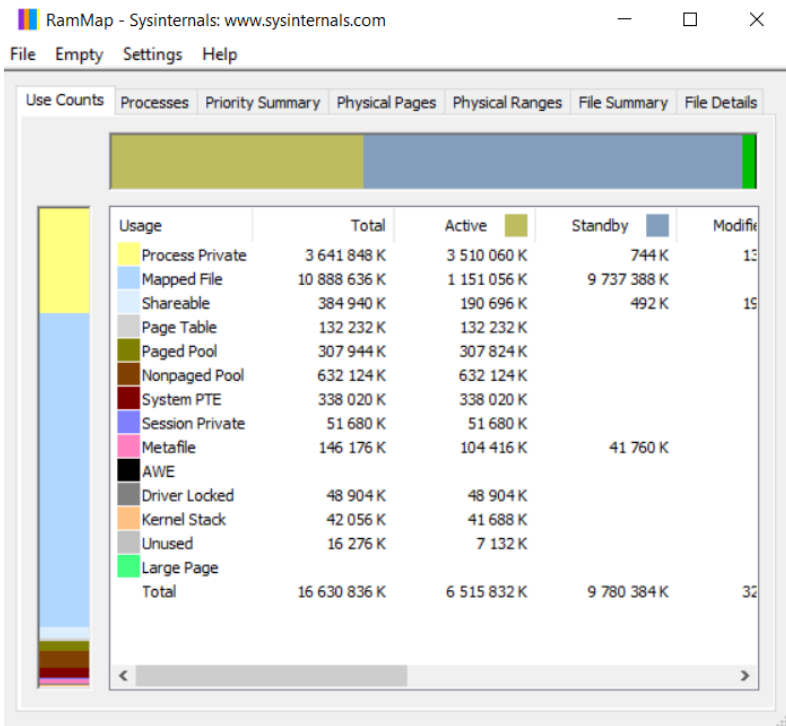
A processzorral kihasználtságáról nyújt információt.

d.) LogonSession

Nem akart elindulni a program, csak egy pillanatra felvillant a tálcán az ikonja majd eltűnt.

A bejelentkezési adatokat mutatná ki.

e.) RAMMap



Memória kihasználtságot mutatja.

3.

a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből

The screenshot shows the Dependency Walker window for EEOAN.EXE. The 'Kernel32.dll' entry is selected in the left pane. The right pane displays a list of API calls with their ordinal, hint, function name, and entry point.

Ordinal	Hint	Function	Entry Point
269 (0x010D)		DeleteCriticalSection	Not Bound
305 (0x0131)		EnterCriticalSection	Not Bound
536 (0x0218)		GetCurrentProcess	Not Bound
537 (0x0219)		GetCurrentProcessId	Not Bound
541 (0x021D)		GetCurrentThreadId	Not Bound
610 (0x0262)		GetLastError	Not Bound
722 (0x02D2)		GetStartupInfoA	Not Bound
747 (0x02E8)		GetSystemTimeAsFileTime	Not Bound
775 (0x0307)		GetTickCount	Not Bound
864 (0x0360)		InitializeCriticalSection	Not Bound
952 (0x03B8)		LeaveCriticalSection	Not Bound
1094 (0x0446)		QueryPerformanceCounter	Not Bound
1180 (0x049C)		SetFilePointer	Not Bound
1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020080
4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x0001B700
5 (0x0005)	4 (0x0004)	AddAtomA	0x0005A140
6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025640
8 (0x0008)	7 (0x0007)	AddConsoleAliasW	0x00025650
9 (0x0009)	8 (0x0008)	AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
10 (0x000A)	9 (0x0009)	AddIntegrityLabelToBoundaryDescriptor	0x0003CCE0
11 (0x000B)	10 (0x000A)	AddLocalAlternateComputerNameA	0x0005A280
12 (0x000C)	11 (0x000B)	AddLocalAlternateComputerNameW	0x0005A2E0

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról!

The screenshot shows the Dependency Walker window for EEOAN.EXE. The 'NTDLL.dll' entry is selected in the left pane. The right pane displays a list of API calls with their ordinal, hint, function name, and entry point.

Ordinal	Hint	Function	Entry Point
8 (0x0008)	N/A	N/A	Not Bound
20 (0x0014)		CsrAllocateCaptureBuffer	Not Bound
21 (0x0015)		CsrAllocateMessagePointer	Not Bound
22 (0x0016)		CsrCaptureMessageBuffer	Not Bound
23 (0x0017)		CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
26 (0x001A)		CsrClientCallServer	Not Bound
27 (0x001B)		CsrClientConnectToServer	Not Bound
28 (0x001C)		CsrFreeCaptureBuffer	Not Bound
29 (0x001D)		CsrGetProcessId	Not Bound
34 (0x0022)		DbgPrint	Not Bound
35 (0x0023)		DbgPrintEx	Not Bound
40 (0x0028)		DbgUiConnectToDbg	Not Bound
41 (0x0029)		DbgUiControl	Not Bound
8 (0x0008)	N/A	N/A	0x0007F110
9 (0x0009)	0 (0x0000)	A_SHAFinal	0x00040230
10 (0x000A)	1 (0x0001)	A_SHAInit	0x00041060
11 (0x000B)	2 (0x0002)	A_SHAUpdate	0x000410A0
12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000E0740
13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x00070620
14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000E0770
15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes	0x000E0790
16 (0x0010)	7 (0x0007)	AlpcGetHeaderSize	0x00070350
17 (0x0011)	8 (0x0008)	AlpcGetMessageAttribute	0x00070310
18 (0x0012)	9 (0x0009)	AlpcGetMessageFromCompletionList	0x0010A60
19 (0x0013)	10 (0x000A)	AlpcGetOutstandingCompletionListMessageCount	0x00085CA0