

Windows Platformunda Bellek ve Performans Analizi

Hasan Mutlu

hasan@hasanmutlu.com

<http://www.hasanmutlu.com/>

2016

Ankara

Windows Platformunda Bellek ve Performans Analizi

- 2001 yılında İstanbul Teknik Üniversitesi Şehir ve Bölge Planlama bölümünden mezun oldum. 2006 yılında İTÜ Gayrimenkul Geliştirme bölümünde yüksek lisans bitirdim.
- Mühendislik yazılımlarına olan ilgim sebebiyle üniversitede okurken programlama ve yazılım geliştirme ile ilgilendim ve kendimi bu konuda geliştirdim. Microsoft geliştirici (MCAD) sertifikası aldım.
- 2001 yılından itibaren yazılım uzmanı olarak çalışıyorum. 2001-2004 yılları arasında İstanbul Büyükşehir Belediyesi Bilgiişlem'inde, 2004-2005 yıllarında Easylink Data Services'de, son 10 yıldır Netcad şirketinde çalışıyorum.
- Uzmanlık alanlarım: Mühendislik yazılımları, geometri - graf algoritmaları, coğrafi bilgi sistemler, ofis programlaması, kentsel model yazılımları. Genelde C# ve Delphi programlama dillerini kullanıyorum.

Windows Platformunda Bellek ve Performans Analizi

- Amaç: Windows platformunda uygulamaların çökmesine, askıda kalmasına, bellek sızıntısı ve performans kaybı yaşamasına neyin sebep olduğunu bulmamıza yardımcı olacak araçlar tanıtılacak ve bu araçlar örneklerle incelenecektir.

Windows Platformunda Bellek ve Performans Analizi

- İlgili araçları anlayabilmek için bazı teknik terimler açıklanacaktır.

Windows Platformunda Bellek ve Performans Analizi

- Program : Statik talimat dizisidir.
- Proses (Process) : Programın çalışan bir örneğidir. Program çalışırken kullandığı kaynakları kapsayan bir yapıdır. Proses aşağıdakileri kapsar:
 - Özel sanal bellek alanı (private virtual address space)
 - Çalıştırılabilir program
 - Çeşitli sistem kaynaklarının açık handle ları (dosyalar, portlar vb..) Bu kaynaklara bütün threadler erişebilir.
 - Güvenlik bağlamı (security context) access token. Bu bilgi kullanıcıyı, grup ve haklarını tanımlar.
 - Proses id. Sistem içinde benzersizdir.
 - En az bir thread

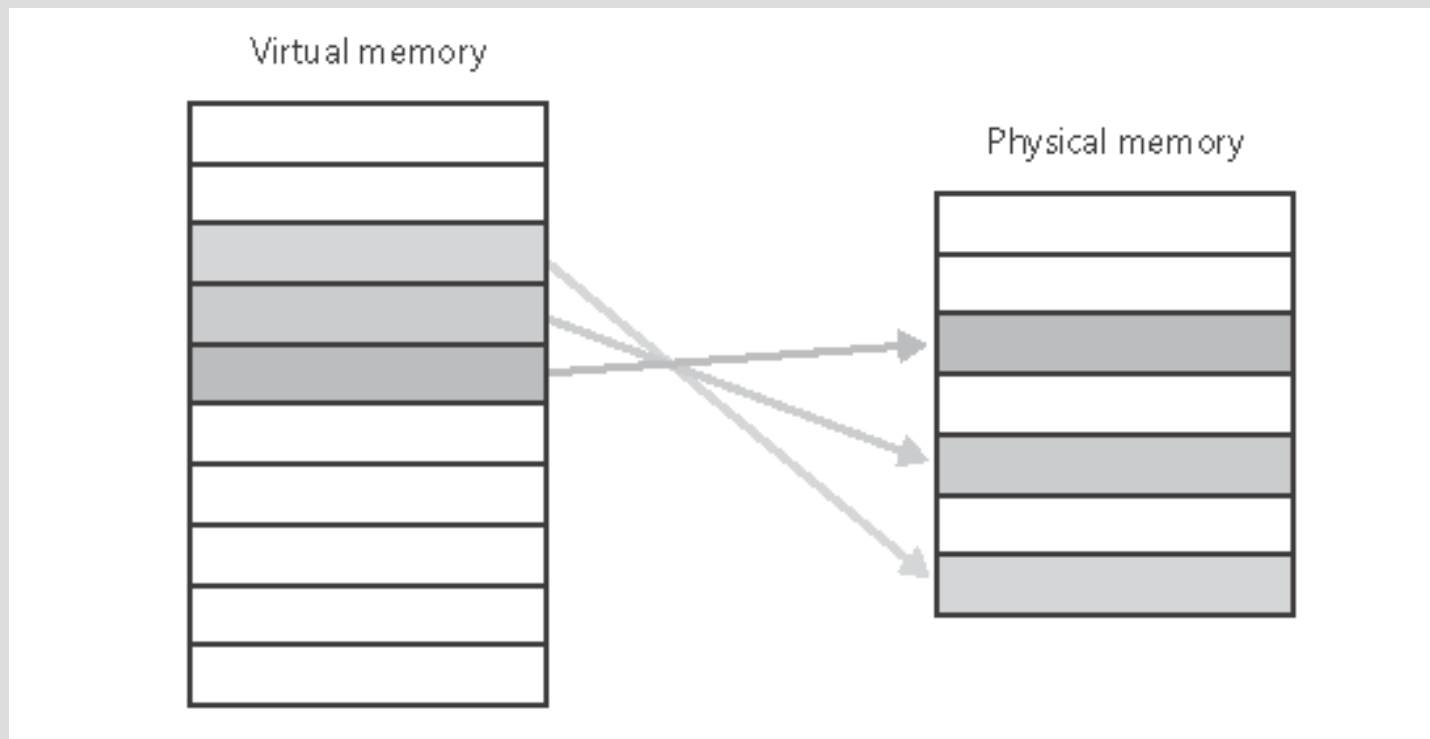
Windows Platformunda Bellek ve Performans Analizi

- İş Parçacığı (Thread) : Bağımsız olarak yönetebilen en küçük program talimat dizisidir. Proses, thread yok ise çalışmaz. Thread aşağıdaki bileşenlerden oluşur:
 - İşlemcinin durumunu bildiren CPU registers.
 - Kernel mod ve user mod için iki yığın (stack)
 - Alt sistemlerin, dll lerin kullanımını için özel depolama alanı (TLS)
 - Benzersiz thread id
 - Bazen kendi güvenlik bağlamı bulunabilir.
- Registers, stack ve TLS bilgisine threadin bağlamı (context) denir. Her threadin kendi çalışma contexti olmasına rağmen process içindeki her thread process in sanal bellek alanını ve processe ait olan kaynakları kullanır. Bu demektir ki her thread bir diğer threadin belleğini okuyabilir ve yazabilir.

Windows Platformunda Bellek ve Performans Analizi

- Sanal Bellek (Virtual Memory) : Windows işletim sistemi, her process için özel, büyük, doğrusal bir bellek alanı olduğu izlenimini yaratır. Bu özel bellek alanına sanal bellek adı verilir. Çalışma zamanında bellek yöneticisi, donanımın da yardımıyla, sanal bellek adresini aslında verinin asıl saklandığı gerçek bellek adresine dönüştürür. İşletim sistemi yaptığı kontrollerle process lerin diğer bir processin veya işletim sistemi verisinin üzerine yazmamasını sağlar.

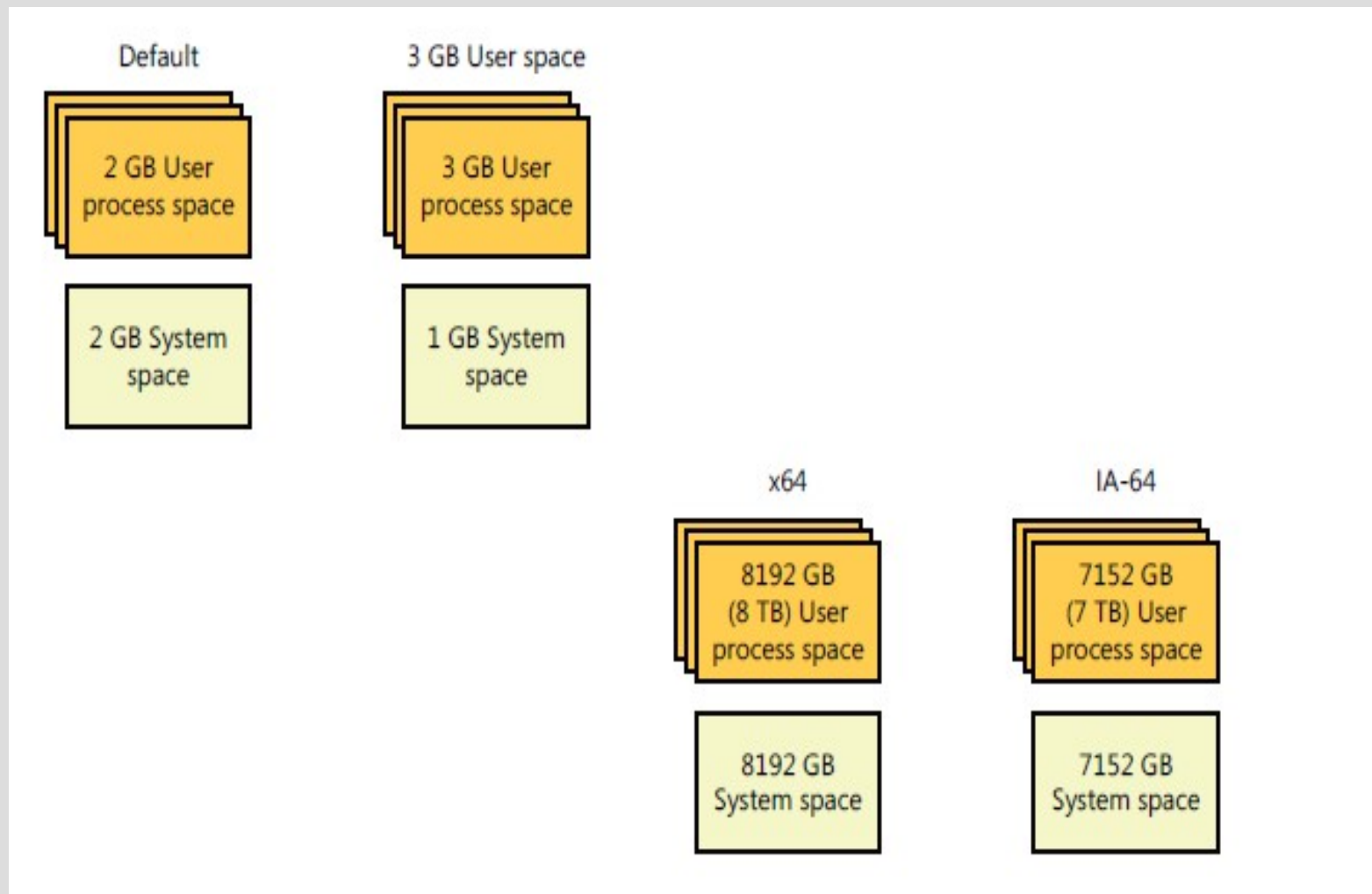
Windows Platformunda Bellek ve Performans Analizi



Windows Platformunda Bellek ve Performans Analizi

- Çoğu sistemde kullanımda olan toplam sanal bellek miktarı, toplam fiziksel bellek miktarından fazla olduğu için bellek yöneticisi bazı bellek içeriklerini diske transfer eder. Bu işleme sayfalama (paging) adı verilir. Diske yapılan sayfalama, fiziksel belleği boşaltır böylece fiziksel bellek diğer bir çalışan process veya işletim sistemi için kullanılabilir duruma gelir. Bir thread diske transfer edilmiş bir sanal bellek adresine erişmeye çalışırsa, bellek yöneticisi diskteki içeriği fiziksel belleğe geri aktarır.
- Sanal bellek adres alanı kapasitesi donanıma-platforma göre değişir. 32 bit x-86 sistemlerde bu alan teorik olarak maksimum 4GB dır. Windows bu bellek alanının yarısını (x00000000 - x7FFFFFFF arası) prosesin özel kullanımına ayırır, diğer yarısını da işletim sisteminin kullanımına ayırır. (Windows ayar değişikliği ile proses alanının 3GB olması mümkün olabilir.)
- 64 bit Windows, prosesler için daha fazla sanal bellek adresi sağlar.(7152 GB Itanium sistemlerde, 8192 GB x64 sistemlerde)

Windows Platformunda Bellek ve Performans Analizi



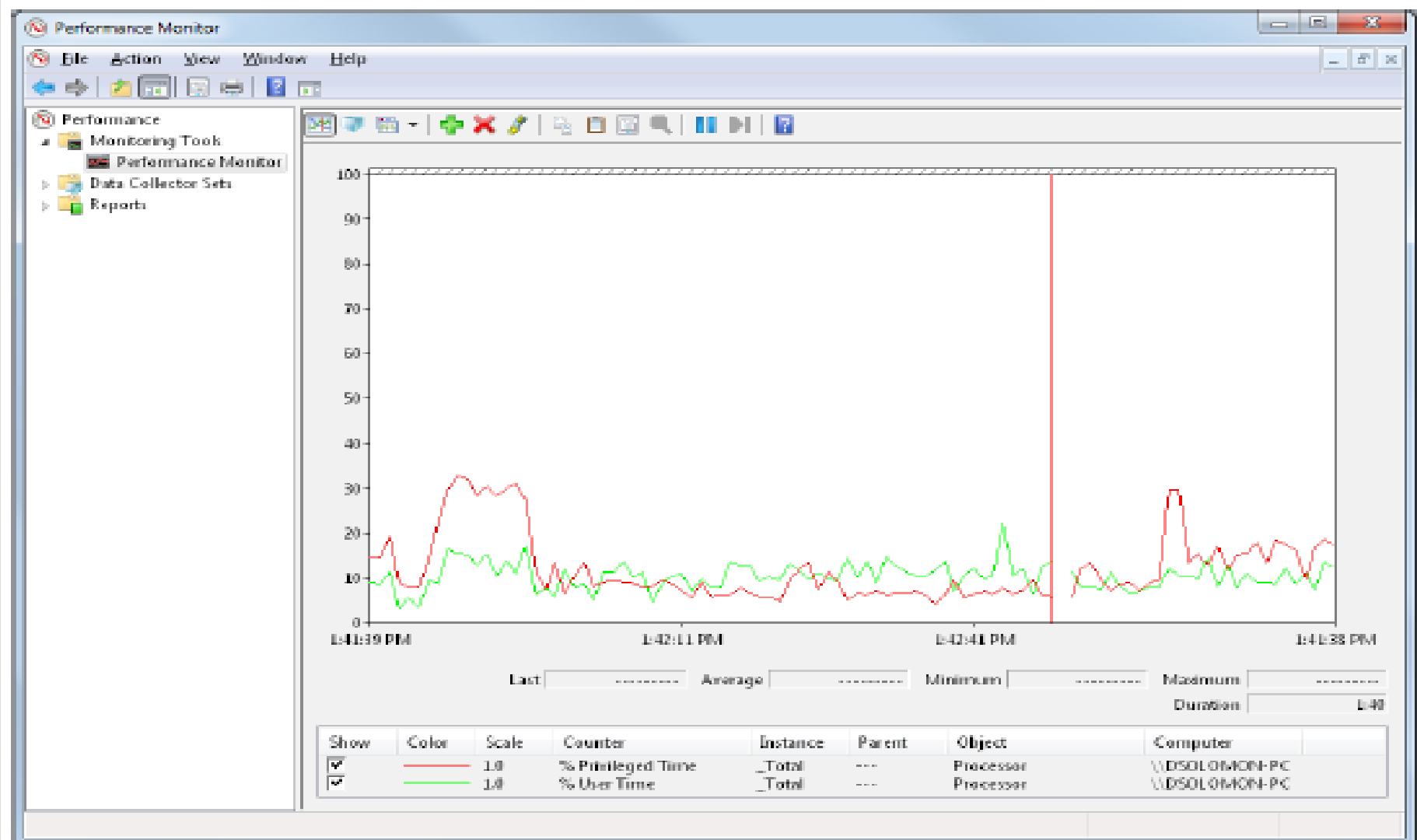
Windows Platformunda Bellek ve Performans Analizi

- Kernel Mod ve User Mod: Kullanıcı uygulamalarının kritik işletim sistemi verilerini bozmaması için Windows 2 tane işlemçi erişim modu kullanır: kullanıcı modu (user mode) ve çekirdek mod(kernel mode).
- Kullanıcı uygulamaları kullanıcı modunda çalışır, işletim sistemi kodları (sistem servisleri, aygıt sürücülerini gibi) çekirdek modda çalışır. Çekirdek modunda, işlem bütün sistem belleğine erişebilir ve tüm işlemçi komutlarını kullanabilir. Kullanıcı uygulaması bu kritik verilere ve işlemlere erişemediği için hatalı bir uygulamanın sistemi bozması engellenmiş olur.
- Windows, çekirdek modu uygulamalarının, sistem belleğine erişimi ile ilgili bir koruma uygulamadığı için bu tip uygulamaların çok dikkatli bir şekilde hazırlanması ve test edilmesi gerekir.

Windows Platformunda Bellek ve Performans Analizi

- Kullanıcı uygulamaları sistem servis çağrısı yaptıklarında kullanıcı modundan çekirdek moda geçerler. Mesela ReadFile metodu içsel veri yapılarına erişmesi gerektiği için çekirdek modda çalışmalıdır. Bu mod geçişi özel bir işlemçi komutu ile çalışır ve işlemçinin çalışma modunu değiştirir. İşletim sistemi bu komutu yakalar, threadin sistem fonksiyonuna gönderdiği parametreler doğrulanır ve içsel fonksiyon çalıştırılır. Kontrol threade dönmeden önce işlemçi tekrar kullanıcı moduna geçer.
- Mesela windows işlemleri, grafik işlemleri çekirdek modda çalıştığı için uygulamaların mod geçişleri performans araçları ile görülebilir. Performans sayaçlarında işlemcinin ve prosesin ayrıcalıklı zaman (privileged time) yüzdesi çekirdek modda geçen süreyi, kullanıcı zaman (user time) yüzdesi kullanıcı modunda geçen süreyi belirtir.

Windows Platformunda Bellek ve Performans Analizi



Windows Platformunda Bellek ve Performans Analizi

- **Objeler ve Tutamaçlar (Objects and Handles) :** Windows işletim sisteminde obje, (object) statik olarak tanımlanmış obje tipinin çalışan bir örneğidir. Obje tipi, sistemi genelinde kullanılan veri tipini, bu tipe uygulanabilecek fonksiyonları ve özellikleri içerir. Mesela proses, thread, dosya, event objeleri gibi örnekler verilebilir.
- **Obje ile veri yapısı arasındaki en önemli fark** objenin içsel yapısının gizli olmasıdır. Objenin içindeki veri yapısına doğrudan erişilemez. Bir obje servisi aracılığıyla bu veriye erişmek gerekir. Bu davranış objenin uygulamasının daha kolay değiştirilebilmesini sağlar. Bütün veri yapıları obje değildir. Sadece paylaşılan, korunmuş, isimlendirilmiş veya kullanıcı modu erişime açılmış veri yapıları obje içinde yer alır.

Windows Platformunda Bellek ve Performans Analizi

- Objelerin kullanımının işletim sistemi için aşağıdaki avantajları vardır:
 - Sistem kaynaklarına anlamlı bir isimle erişilebilmesi
 - Prosesler arası kaynak ve veri paylaşılabilirliği
 - Kaynakların yetkisiz erişimden korunması
 - Referans izleme, hangi objenin kullanım dışı kaldığının belirlenip, yok edilebilmesi

Windows Platformunda Bellek ve Performans Analizi

- Tanıtılacak Araçlar
 - Prosesin Çalışması İle İlgili Sorunlar : Process Explorer – Process Monitor
 - Windows Kontroller ve Mesaj Sistemi İle İlgili Sorunlar - Spyxx
 - Bellek Sorunları – Performans İzleyicisi - VMMap – Windbg
 - Performans Sorunları - Debug Diagnostic Tool

Windows Platformunda Bellek ve Performans Analizi

- Process Explorer : Ücretsiz ve kurulum gerektirmeyen bir görev yönetici programıdır. Standart görev yöneticisinin tüm özelliklerinin yanında, gelişmiş dll ve exe takipçisi, CPU, Commit, RAM, I/O, Ağ ve Disk kullanımının görüntülenebileceği gelişmiş bir yöneticidir.
- Ayrıca proseslerin yüklediği dlleri ve açık handle larını da gösterebildiği için dll yükleme ve handle kaçağı (handle leak) ile ilgili sorunların çözümüne yardımcı olur.
- <https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx>

Windows Platformunda Bellek ve Performans Analizi

The screenshot displays the Process Explorer application window. The main pane shows a list of processes with columns for CPU usage, Private Bytes, Working Set, PID, Description, Company Name, and USER Objects. The 'Bellek_PerfTest.exe' process is highlighted in cyan, showing a CPU usage of 0.13, 16,376 K Private Bytes, and 39,108 K Working Set. Below the process list, the 'System Objects' pane shows a list of system objects, including Window Stations, Threads, Sections, and Mutants, with the selected object being '\Sessions\1\Windows\WindowStations\WinSta0'. The status bar at the bottom indicates CPU Usage: 2.95%, Commit Charge: 23.62%, Processes: 123, and Physical Usage: 62.30%.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	USER Objects
chrome.exe		1,804 K	9,172 K	8624	Google Chrome	Google Inc.	4
chrome.exe	< 0.01	26,288 K	38,884 K	8604	Google Chrome	Google Inc.	13
chrome.exe	< 0.01	53,764 K	62,244 K	8780	Google Chrome	Google Inc.	0
chrome.exe	< 0.01	56,608 K	68,020 K	1652	Google Chrome	Google Inc.	0
chrome.exe	< 0.01	31,880 K	40,724 K	6220	Google Chrome	Google Inc.	0
chrome.exe	0.04	77,328 K	103,380 K	10068	Google Chrome	Google Inc.	0
chrome.exe	0.02	58,456 K	73,108 K	5572	Google Chrome	Google Inc.	0
Taskmgr.exe	0.13	16,376 K	39,108 K	9180			508
procexp64.exe	1.06	26,072 K	67,844 K	5948	Sysinternals Process Explorer	Sysinternals - www.sysinter...	293
Bellek_PerfTest.exe		15,648 K	20,636 K	7300	Bellek_PerfTest		24
LManager.exe	0.01	3,624 K	11,264 K	560	Launch Manager	Ditek System Inc.	15
MMDx64Fx.exe		2,332 K	10,480 K	6248	MMDx64Fx Application	Ditek System Inc.	7
lirfxEM.exe							

Type	Name
Window Station	\Sessions\1\Windows\WindowStations\WinSta0
Window Station	\Sessions\1\Windows\WindowStations\WinSta0
Thread	Bellek_PerfTest.exe(7300): 5632
Thread	Bellek_PerfTest.exe(7300): 10164
Thread	Bellek_PerfTest.exe(7300): 5472
Thread	Bellek_PerfTest.exe(7300): 5472
Thread	Bellek_PerfTest.exe(7300): 10164
Thread	Bellek_PerfTest.exe(7300): 6280
Section	\Sessions\1\BaseNamedObjects\SessionImmersiveColorPreference
Section	\Sessions\1\Windows\Theme4172760624
Section	\Windows\Theme1971974456
Section	\BaseNamedObjects\Cor_Private_IPCBlock_v4_7300
Section	...\Cor_SxSPublic_IPCBlock
Mutant	\Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1S-1-5-21-3436755411-517567...
Mutant	\Sessions\1\BaseNamedObjects\SessionImmersiveColorMutex

CPU Usage: 2.95% | Commit Charge: 23.62% | Processes: 123 | Physical Usage: 62.30%

Windows Platformunda Bellek ve Performans Analizi

- Process Monitor : Windows sistemindeki bazı aktivitelerin gerçek zamanlı olarak izlenebilmesini sağlayan araçtır.
- <https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx>
- İzlenen aktiviteler:
 - Dosya sistemi
 - Registry
 - Process - thread : Proses -thread in başlaması, sonlandırılması. Yüklenen dlller ve driver ların bilgisi izlenebilir.
 - Network : ETW (Event Tracing For Windows) kullanarak TCP ve UDP aktivitesini izler. Kaynak ve varış adresleri, ne kadar büyüklükte veri akışı olduğu gibi bilgiler izlenir. Ancak verinin içeriği gözükmez.
 - Proses Profiling : Proses hakkında bazı bilgiler. Kernel ve user time. Private bytes gibi.

Windows Platformunda Bellek ve Performans Analizi

- Bu araç aktiviteleri esnek bir şekilde filtrelemenizi sağlayarak sorunu kolay bir şekilde incelemenizi sağlar. Kolonları seçerek ilgili aktivite için istenen bilgilerin gösterilmesi sağlanabilir. Önemli kolonlar şunlardır:
 - Process Name: Uygulama adı
 - Time Of Day : Olayın oluştuğu zaman
 - PID : Proses id
 - Operation : Olayın adıdır. Çok çeşitli değerler olabilir. (CreateFile, CloseFile gibi.) (Filtreden incelenebilir.)
 - Path : Olayla ilgili dosya yoludur.
 - Result : Olayın sonuç durumudur.
 - Detail : Olayla ilgili detay bilgiler.

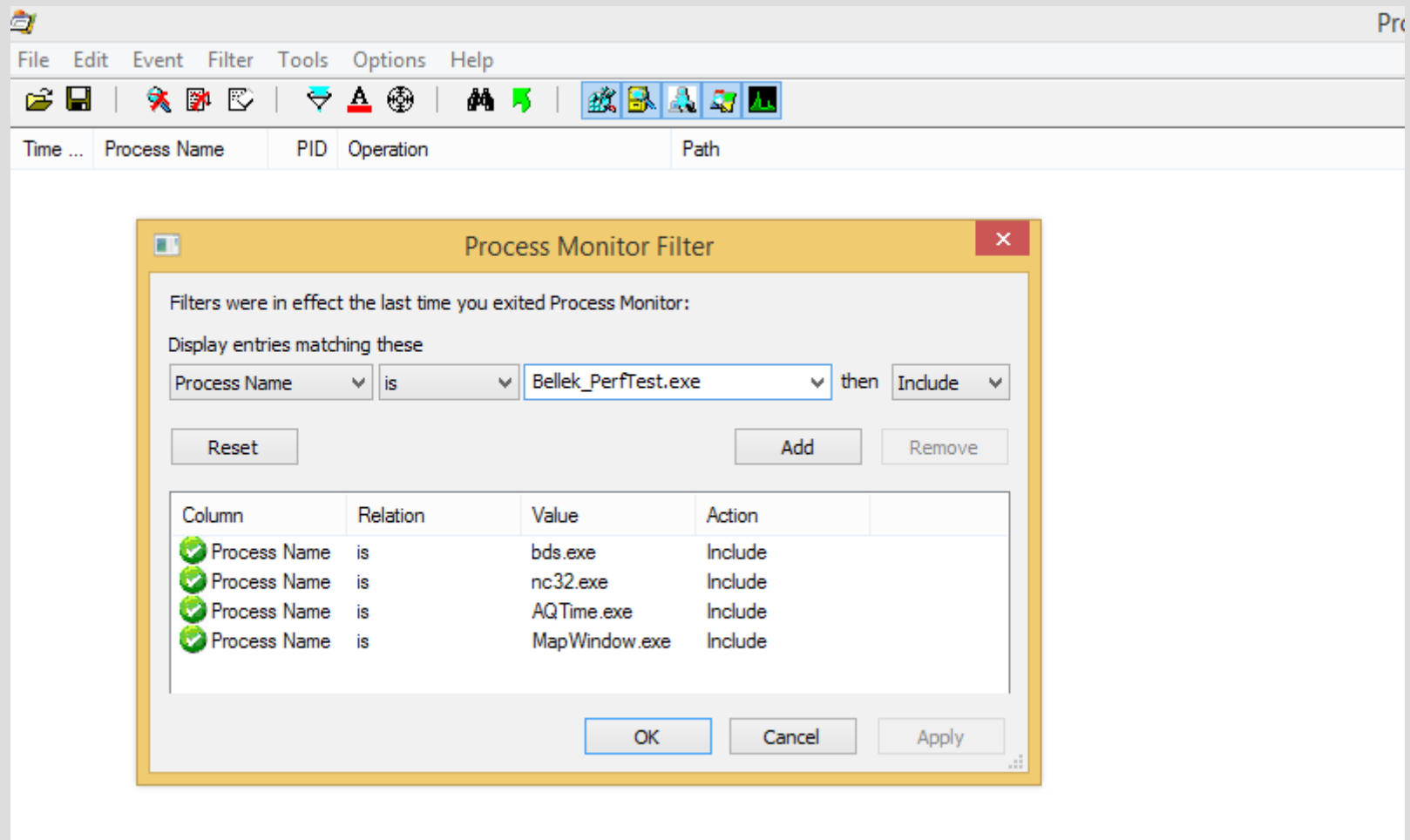
Windows Platformunda Bellek ve Performans Analizi

- Uygulamanın üstündeki toolbox daki butonlar ile hangi tür aktivitenin izleneceđi belirlenebilir.

Windows Platformunda Bellek ve Performans Analizi

- Örnek senaryoda program bir dosyaya erişmek istiyor olsun. Ancak bu dosya bulunmadığı için oluşan hatayı bulmak isteyelim.
- Bu durumda ilgili program adını filtreye ekleriz. Daha sonra programı çalıştırıp process monitor programının sonuçlarını inceleriz.

Windows Platformunda Bellek ve Performans Analizi



The image shows a screenshot of the Windows Process Monitor application with a 'Process Monitor Filter' dialog box open. The dialog box displays the filters currently in effect. The main window behind the dialog shows a table with columns: Time ..., Process Name, PID, Operation, and Path.

Process Monitor Filter

Filters were in effect the last time you exited Process Monitor:

Display entries matching these

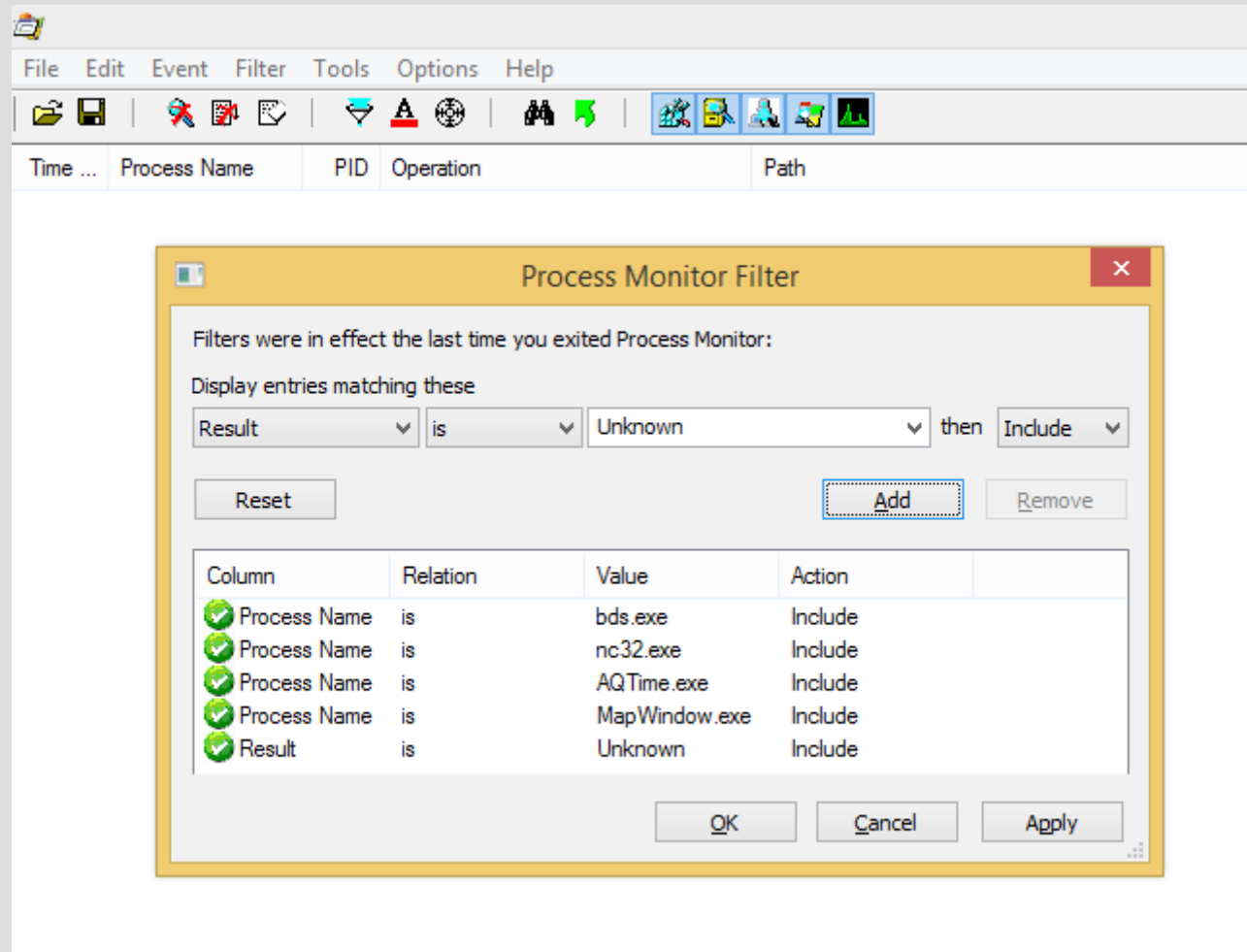
Process Name is Bellek_PerfTest.exe then Include

Reset Add Remove



Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	bds.exe	Include
<input checked="" type="checkbox"/> Process Name	is	nc32.exe	Include
<input checked="" type="checkbox"/> Process Name	is	AQTime.exe	Include
<input checked="" type="checkbox"/> Process Name	is	MapWindow.exe	Include

OK Cancel Apply

Windows Platformunda Bellek ve Performans Analizi



Windows Platformunda Bellek ve Performans Analizi

ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
is Help			
			
on	Path	Result	Detail
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ueryKey	HKLM	SUCCESS	Query: HandleTa
ueryKey	HKLM	SUCCESS	Query: Name
penKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: F
ss Profiling		SUCCESS	User Time: 0.187
ueryKey	HKLM	SUCCESS	Query: HandleTa
ueryKey	HKLM	SUCCESS	Query: Name
penKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: F
File	D:\hasan\HasanE\calismalar\geciciProje\Bellek_PerfTest\Bellek_PerfTest\bin\Debug\deneme.txt	NAME NOT FOUND	Desired Access: C
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187
is Help			
			
on	Path	Result	Detail
ss Profiling		SUCCESS	User Time: 0.187
ss Profiling		SUCCESS	User Time: 0.187

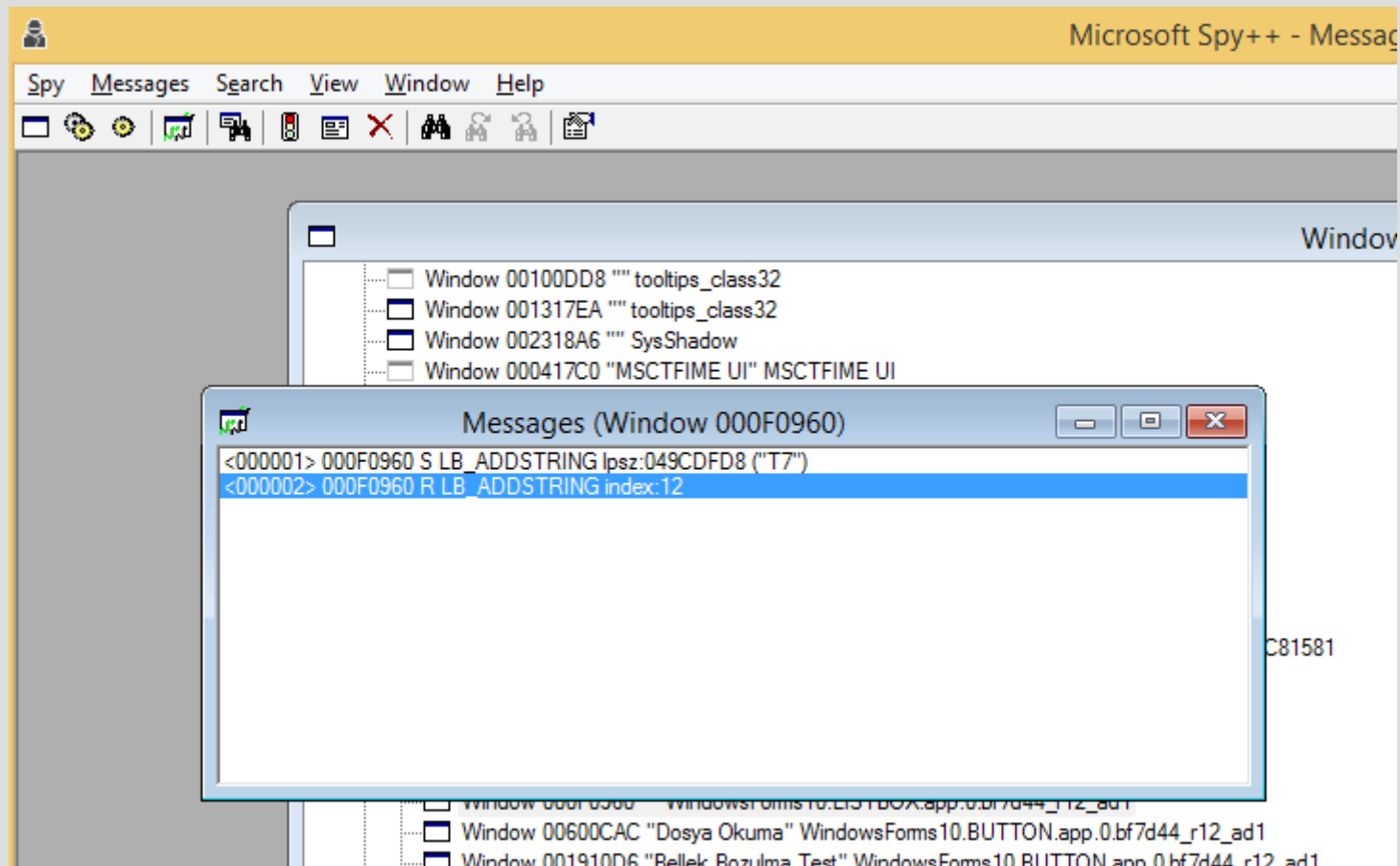
Windows Platformunda Bellek ve Performans Analizi

- Spyxx : Sistemdeki prosesler, iş parçacıkları (thread), pencereler (window) ve windows mesajları ile ilgili bilgiler verir. Bu objeler arasındaki ilişkilerin grafiksel olarak görülebilmesini sağlar. Visual Studio ile gelir.
- Özellikle windows mesaj sistemi ile ilgili önemli bilgiler alınabildiği için kullanıcı arayüzü ile ilgili problemlerin sorunlarının çözülmesi için faydalı bir araçtır.
- Mesaj kodları şu şekildedir.
 - P : PostMessage fonksiyonu ile gelen mesajlardır. Bu mesajların sonucunun dönmesi beklenmez.
 - S : SendMessage fonksiyonu ile gelen mesajlardır. Bu mesajı gönderen, işlem bitene kadar bekler. Mesajı alan göndericiye bir dönüş değeri döndürebilir.
 - s : Mesaj gönderildi ama dönüş değeri güvenlik sebebiyle engellendi.
 - R : Dönüş değeri mesajıdır. Her S mesajı bir R mesajı döndürür. İç içe geçmiş mesajlar da olabilir.

Windows Platformunda Bellek ve Performans Analizi

- Spyxx programının çalışması ile ilgili örnek senaryo şöyledir.
 - Bir form uygulaması vardır.
 - Bir buton listboxa T7 değerinde bir değer eklemektedir.
 - Spy++ programı ile ilgili listboxın mesajları incelenir.

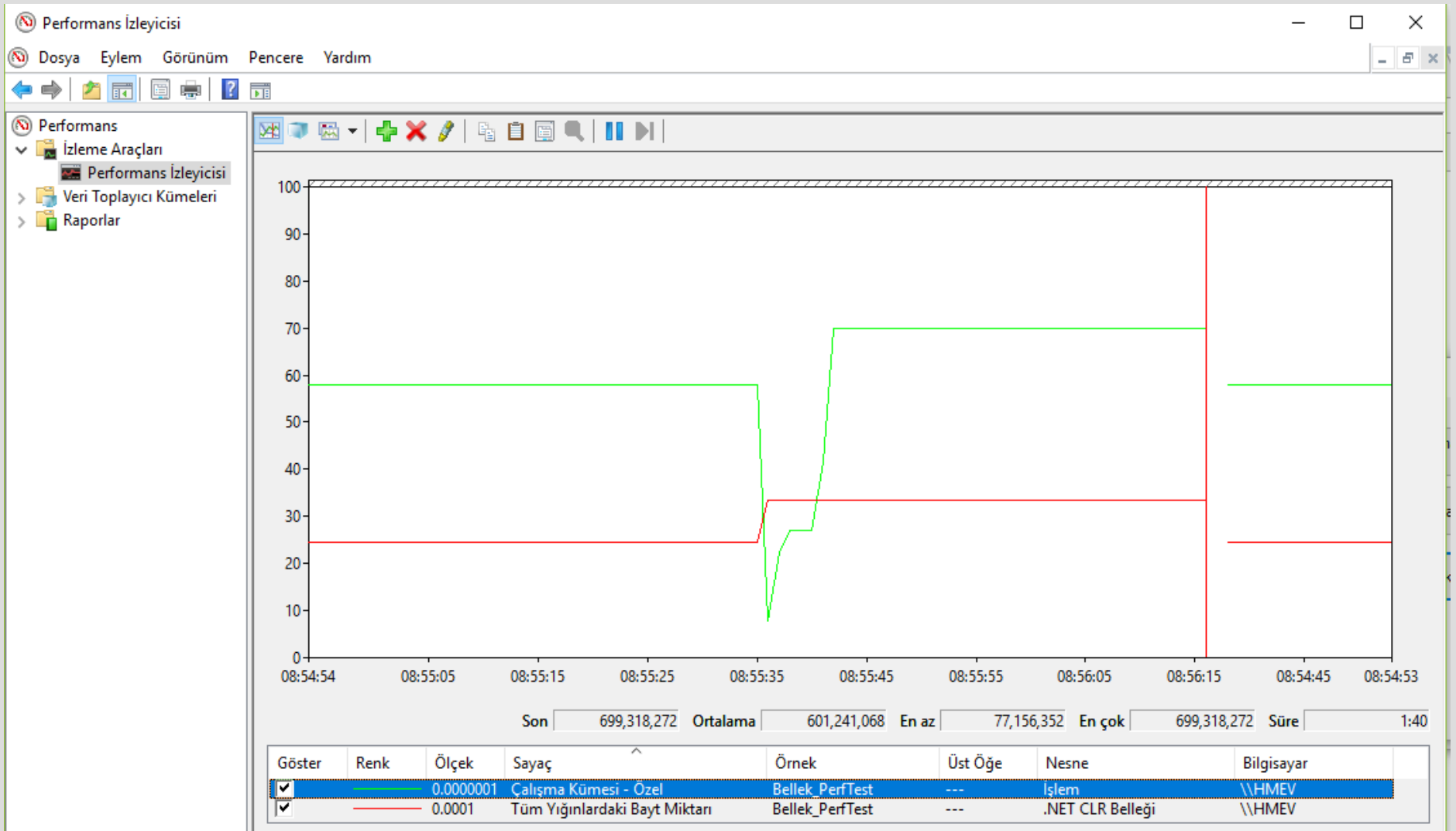
Windows Platformunda Bellek ve Performans Analizi



Windows Platformunda Bellek ve Performans Analizi

- Performans İzleyicisi (perfmon) : Bu uygulama sistem ve proses bazında pek çok değişik türde sayacın (bellek, işlemci zamanı vb..) gerçek zamanlı izlenebileceği güçlü bir araçtır. Windows ile gelir.
- Bu aracı kullanarak bir prosesde bellek kaçağı olup olmadığını hızlıca kontrol edebiliriz. Managed heap kontrol etmek için .NET CLR Belleği / Tüm Yığınlardaki Bayt Miktarı sayacını, unmanaged heap kontrol etmek için İşlem / Çalışma Kümesi Özel sayaçlarını ilgili proses için eklememiz gerekir.
- Daha sonra uygulamamızı çalıştırıp sayaçları inceleyerek uygulamamızın bellek sorunu yaşayıp yaşamadığı belirlenebilir.
- https://www.codeproject.com/kb/dotnet/memory_leak_detection.aspx

Windows Platformunda Bellek ve Performans Analizi



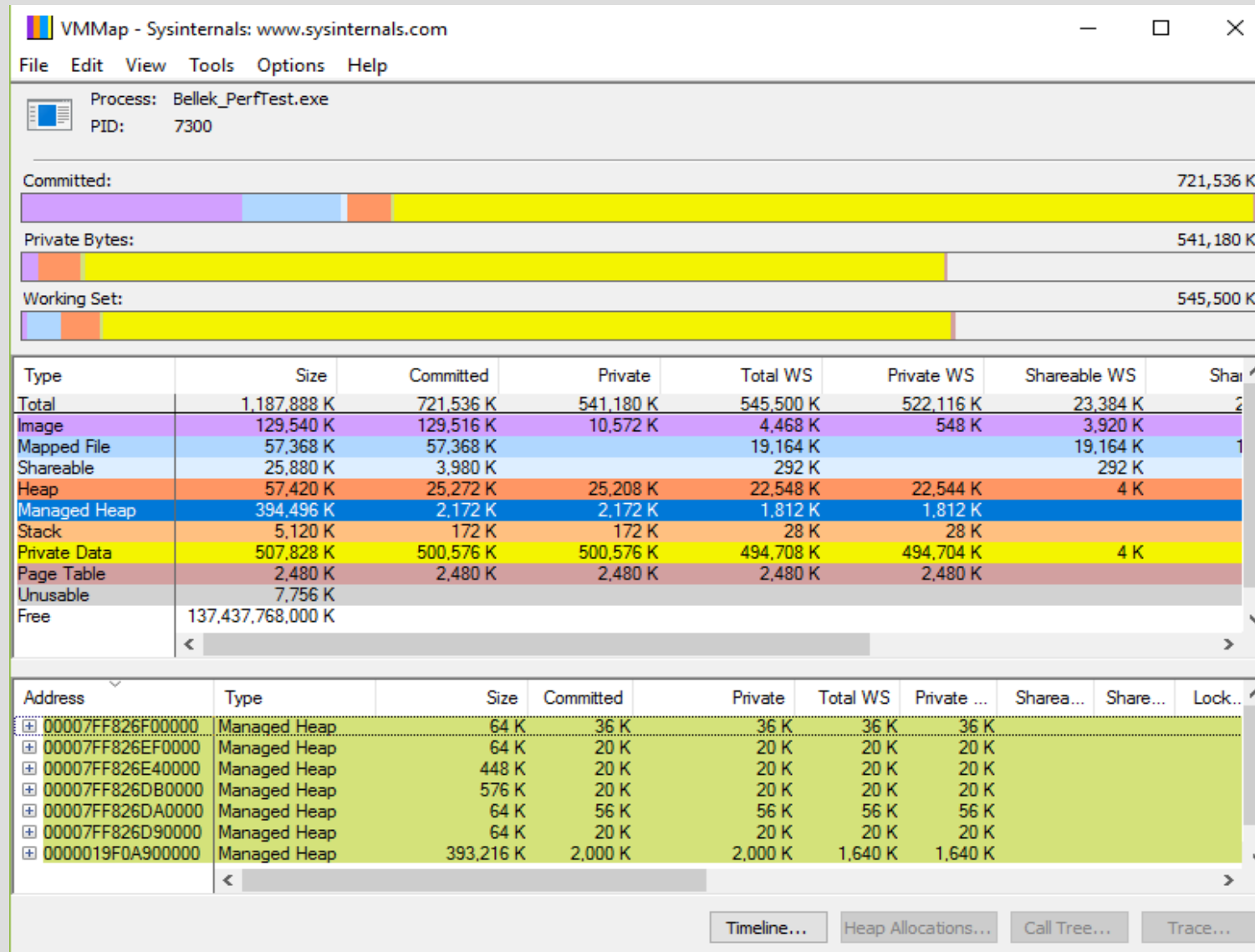
Windows Platformunda Bellek ve Performans Analizi

- VMMap : Bir prosesin sanal ve fiziksel bellek kullanımını analiz etmeye yarayan bir araçtır. Bellek türleri buldukları bellek bölümüne göre gösterilirler.
- Bellek Bölümleri:
 - Committed : Sanal bellekte kullanılır durumdaki bayt miktarıdır. Bu miktar sadece sayfalama için kullanılan miktar değildir. Fiziksel bellekte bulunan ve hiç sayfalama yapılmayacak bölümü de içerir.
 - Private Bytes : Uygulamanın sadece kendinin kullandığı paylaşılmayan bellek miktarıdır. Bu bellek fiziksel bellekte de yer alabilir, sayfalama yapısında da bulunabilir.
 - Working Set : Proses tarafından kullanılan fiziksel bellek miktarıdır.

Windows Platformunda Bellek ve Performans Analizi

- Bellek Türleri:
 - Image : Çalışabilir kodu temsil eder. Modülün yüklediği dll , exe.
 - Mapped File : Diskteki bir dosyayı temsil eder. Uygulama verileri genelde burada bulunur.
 - Shareable : Diğer prosesler ile veri paylaşabilen bellek.
 - Heap : Kullanıcı mod heap yöneticisi tarafından yönetilen bellek
 - Managed Heap : Garbage Collector tarafından kontrol edilen .NET heap
 - Stack : Thread in çalışması sırasında tuttuğu fonksiyon içi değişken, adres gibi değişkenleri içerir.
 - Private Data : Uygulamaya özel verilerdir. (heap, managed heap ve stack da yer almayan)
 - Page Table : Prosesle ilişkili kernel mode sistem belleğidir. Fiziksel bellekte yer alır.
 - Unusable : Boş olan ancak bazı kısıtlardan dolayı kullanılmayan sanal bellek miktarıdır.

Windows Platformunda Bellek ve Performans Analizi



Windows Platformunda Bellek ve Performans Analizi

- WinDbg :Microsoft tarafından geliştirilmiş çok amaçlı debuggerdır. Windows Sdk ile sisteme kurulur. Oldukça gelişmiş özellikleri vardır, dump dosyaları ile çöküş sonrası hata ayıklama (post-mortem debugging) yapabilir.
- <https://en.wikipedia.org/wiki/WinDbg>
- Örnek olarak bu araç kullanılarak bir .NET uygulamasındaki bellek kullanımını analiz edilecektir.
 - İlgili uygulamaya bağlanılır. (Attach To Process)
 - Uygulama .NET bileşeni olduğu için “.load sos” komutu ile SOS bileşeni yüklenir. (Uygulamanın .NET Framework versiyonuna göre komut değişik olabilir. .NET 2.0 için “.loadby sos mscorwks” , 4.0 için “.loadby sos clr” da kullanılabilir.)
 - “!DumpHeap -stat” komutu ile açık olan .NET objeleri tipleri ile ilgili istatistiki bilgiler alınır.

Windows Platformunda Bellek ve Performans Analizi

- “!DumpHeap -type System.Windows.Forms.Button” komutu ile verilen tipteki objeler listelenir.
- “!dumpheap -mt ” komutu ile bu obje tipindeki bütün objelerin adresleri listelenecektir.
- “!gcroot ” komutu ile bu objeyi yükleyen ve saklayan yapılar hakkında bilgi alınabilir.

Windows Platformunda Bellek ve Performans Analizi

- Debug Diagnostic Tool : Kullanıcı uygulamalarının askıda kalma, çökme, düşük performans , bellek sızıntısı gibi sorunlarına yardımcı olmak için geliştirilmiş bir araçtır.
- Kullanımı kısaca şöyledir.
 - DebugDiag 2 Collection programı ile uygulama ile ilgili dump dosyaları oluşturulur.
 - Daha sonra Debug 2 Analysis programı ile bu dump dosyaları analiz yaptırılır. Sonuç raporlar incelenerek sorun hakkında bilgi sahibi olunur.
- <https://www.toptal.com/dot-net/hunting-high-cpu-usage-in-dot-net>

Windows Platformunda Bellek ve Performans Analizi

Teşekkürler...