CERTKILL

Microsoft 70-660

70-660 TS: Windows Internals

Practice Test

Version 1.1

QUESTION NO: 1

You have an application that runs at a customer's site. Sometimes, the application crashes because of heap corruption. You ask the customer to enable full page heap on the application process so that you can troubleshoot the heap corruption.
The customer sends you a user dump file. You need to identify if the full page heap was enabled when the user dump was created. Which WinDbg command should you use?

A. !gflag
B. !heap
C. !verifier
D. !vm

Answer: A

QUESTION NO: 2

You are the IT professional who work in an International company named Wiikigo. You are experienced in troubleshooting operating systems and applications that are not working correctly, identifying code defects and so on. You have enough knowledge on windows internals and you provide technical support for the company. There is a computer named c01. Windows Server 2008 is run by C01. Now you are using WinDbg to debug C01. You find that one thread is waiting for a critical section. This section is owned by another thread. You have to locate the critical section. Of the following WinDbg commands, which one should be used?

A. You should choose to use.thread
B. You should choose to use !deadlock
C. You should choose to use!kdext.locks
D. You should choose to use!ntsdexts.locks

Answer: D

QUESTION NO: 3

You are the IT professional who work in an International company named Wiikigo. You are experienced in troubleshooting operating systems and applications that are not working correctly, identifying code defects and so on. You have enough knowledge on windows internals and you provide technical support for the company. There is a colleague named Jason in the company. He has a computer named C01. C01 runs Windows Vista. He finds that a service process is using 100 percent of the processor. He has to force a process dump of the service, meanwhile the service is consuming 100 percent of the processor. He has no idea about which tool he should use. Since you are the technical support, he asks for your answer. So which of the

following tools should be used?

A. He should choose to use Umdh.exe
B. He should choose to use Tlist.exe
C. He should choose to use Pview.exe
D. He should choose to use Adplus.vbs

Answer: D

QUESTION NO: 4

You are the IT professional who work in an International company named Wiikigo. You are experienced in troubleshooting operating systems and applications that are not working correctly, identifying code defects and so on. You have enough knowledge on windows internals and you provide technical support for the company. According to the company requirement, you are debugging a Windows device driver. An unexpectedly long delay occurs on the device driver. You locate the problem in the following synchronization mechanism.
kd> dt var_sema
Local var @ 0xf9dfbc48 Type _KSEMAPHORE
+0x000 Header : _DISPATCHER_HEADER
+0x010 Limit : 2
kd> dt nt!_DISPATCHER_HEADER f9dfbc48
+0x000 Type : 0x5 ''
+0x001 Absolute : 0xe6 ''
+0x002 Size : 0x5 ''
+0x003 Inserted : 0xbb ''
+0x004 SignalState : 0
+0x008 WaitListHead : _LIST_ENTRY [0x819ca438 - 0x819ca438]
kd> dt nt!_KWAIT_BLOCK 0x819ca438
+0x000 WaitListEntry : _LIST_ENTRY [0xf9dfbc50 - 0xf9dfbc50]
+0x008 Thread : 0x819ca3c8 _KTHREAD
+0x00c Object : 0xf9dfbc48
+0x010 NextWaitBlock : 0x819ca480 _KWAIT_BLOCK
+0x014 WaitKey : 0
+0x016 WaitType : 1
kd> dt nt!_KWAIT_BLOCK 0xf9dfbc50
+0x000 WaitListEntry : _LIST_ENTRY [0x819ca438 - 0x819ca438]
+0x008 Thread : 0x00000002 _KTHREAD
+0x00c Object : 0xfd050f80
+0x010 NextWaitBlock : 0xffffffff _KWAIT_BLOCK
+0x014 WaitKey : 0
+0x016 WaitType : 0

You have to find out the number of threads that the semaphore currently has waiting. How many threads does the semaphore currently have waiting?

A. 0
B. 1
C. 2
D. 4
E. 5

Answer: B

QUESTION NO: 5

You are writing an I/O dispatch routine for a Windows device driver. The device driver supports buffered
I/O. The dispatch routine transfers 1 KB of data to the user process.
You need to retrieve the kernel address of the 1-KB buffer from the I/O request packet (IRP).
Which field of the IRP contains the kernel address?

A. Irp->AssociatedIrp.SystemBuffer
B. Irp->Overlay.UserApcContext
C. Irp->Tail.Overlay.DriverContext[0]
D. Irp->UserBuffer

Answer: A

QUESTION NO: 6

You are the IT professional who work in an International company named Wiikigo. You are experienced in troubleshooting operating systems and applications that are not working correctly, identifying code defects and so on. You have enough knowledge on windows internals and you provide technical support for the company. You are in charge of a multithreaded application. Now is being tested by you. You have to use Perfmon to test the application for heap leaks. Of the following counters, which one should be monitored?

A. Process\Private Bytes
B. Memory\Available Bytes
C. Memory\Committed Bytes
D. Process\Pool Paged Bytes

Answer: A