IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **070-660**

Title : TS:Windows Internals

Version : DEMO

1.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 an application. This application runs at a customer's site. Because of heap corruption, the application crashes intermittently. In order to enable yourself to check and resolve the heap corruption, you ask the customer to have full page heap enabled on the application process. You receive a user dump file from the customer. What you should do is to make it clear at the time that the user dump was created, whether the full page heap was enabled. Of the following WinDbg commands, which one should be used?

A.!vm should be used.

B.!gflag should be used.

C.!heap should be used.

D.!verifier should be used.

Answer:B

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

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

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

5.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, an I/O dispatch routine is being written by you for a Windows device driver. buffered I/O is supported by the device driver. 1 KB of data to the user process is transferred by the dispatch routine. The kernel address of the 1-KB buffer needs to be retrieved from the I/O request packet (IRP). Which field of the IRP contains the kernel address?

A.Irp->UserBuffer

B.Irp->Overlay.UserApcContext

C.Irp->Tail.Overlay.DriverContext[0]

D.Irp->AssociatedIrp.SystemBuffer

Answer:D

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

7.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. For a hardware device, you are developing a Windows device driver. You will install the device driver and hardware device on computers that run Windows Server 2008. Now you have to find out the amount of time that the processor uses to receive and process interrupts. Which of the following tools should be used?

A.You should choose to use Pview.exe

B.You should choose to use Taskmgr.exe

C.You should choose to use Eventvwr.msc

D.You should choose to use Perfmon.msc

Answer:D

8.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 writing a user application that runs on Windows Server 2003. According to the company requirement, a user application is being written by you. This application runs on Windows Server 2003. User authentication is need by the design specification for the application. You must make sure that each time the application is started, a local user name and password is entered by users. So which routine should be used?

A.CredUIParseUserName()should be used.

B.LsaRegisterLogonProcess()should be used.

C.CredReadDomainCredentials() should be used.

D.CredUIPromptForCredentials()should be used.

Answer:D

9.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 have a device driver that has one monitoring thread named ThreadA. The device driver has three worker threads. They are respectively named ThreadB, ThreadC, and ThreadD. The worker threads run every 10 seconds and complete within 1 second. If any worker thread does not run at least once every 30 seconds, ThreadA calls KeBugCheckEx, and then a complete kernel crash dump is generated. A bug check and a complete kernel dump are generated by the computer. You find the following after you review the complete kernel dump: You have to find out the root cause of the bug check. So what caused the bug check to occur?

Thread Name	ThreadA	ThreadB	ThreadC	ThreadD
State	Running	Ready	Ready	Ready
Priority	LOW_REALTIME_PRIORITY	LOW_REALTIME_PRIORITY	LOW_REALTIME_PRIORITY	LOW_PRIORITY

A.It was caused by the state of ThreadA

B.It was caused by the priority of ThreadA.

C.It was caused by the priority of ThreadD

D.It was caused by the state of ThreadA and ThreadB

E.It was caused by the state of ThreadB and ThreadC

Answer:C

10.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 an application service. Because of heap corruption, it crashes intermittently. When it occurs, you have to detect the heap corruption. Of the following tolls, which one should be used?

A.You should choose to use Page Heap

B.You should choose to use Special Pool

C.You should choose to use driver Verifier

D.You should choose to use Memory Pool Monitor

Answer:A