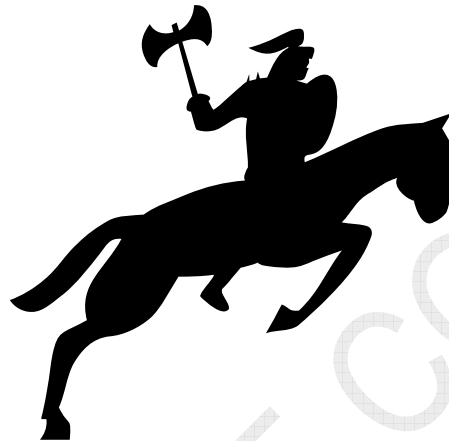


Easy CramBible Lab



70-660

TS:Windows@ Internals

**** Single-user License ****

This copy can be only used by yourself for educational purposes

Web: <http://www.crambible.com/>

E-mail: web@crambible.com

Important Note
Please Read Carefully**Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions.

Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at CramBible an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.CramBible.com
2. Click on Member zone/Log in
3. The latest versions of all purchased products are download from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback

Feedback on specific questions should be send to web@CramBible.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, CramBible reserves the right to take legal action against you according to the International Copyright Laws.

THE TOTAL NUMBER OF QUESTIONS IS 43**QUESTION NO:1**

You have a computer that runs Windows Server 2003. You notice that the total kernel-mode CPU time for the processor is 80 percent, and the total kernel-mode CPU time for all processes is 60 percent.

You need to identify what is using the remaining 20 percent of the kernel-mode CPU time. Which two Perfmon counters should you use? (Each correct answer presents part of the solution. Choose two.)

- A. Processor\% DPC Time
- B. Processor\Interrupts/sec
- C. Processor\% Interrupt Time
- D. System\Context Switches
- E. System\System Calls/sec

ANSWER: AC

QUESTION NO:2

You install and run a new device driver. You receive the following error message.

Event ID: 2020 Source: Srv

Description: The server was unable to allocate from the system paged pool because the pool was empty.

You suspect that a device driver is causing kernel memory pool leaks. You find a kernel memory allocation tag named TAG1 that belongs to the leaked memory. You need to identify the device driver and the corresponding call stack that is causing the memory leak. What should you do?

- A. Run Findstr.exe /m TAG1 *.sys.
- B. Run Findstr.exe TAG1 pooltag.txt.
- C. Use Driver Verifier and enable the Special Pool option.
- D. Use WinDbg to issue the command ed ntlPoolHitTag '1GAT'.

ANSWER: D

QUESTION NO:3

You have a computer that runs Windows Server 2008. The computer crashes weekly and creates a complete memory dump. You run the analyze command from WinDbg and receive the following output:

Bad_Pool_Header 0x0000000019 (0x0000000020, 0xa34583b8, 0xa34584f0, 0x0a270001) You need to identify the pool tag that is associated with the

Bad_Pool_Header pool allocation. Which WinDbg command should you use?

- A. Ipool
- B. Ipoolused
- C. Ivm
- D. Ixpoolmap

ANSWER:A

QUESTION NO:4

You have a computer that runs Windows Vista. The computer intermittently performs slowly. When the computer performs slowly, you notice that the System process uses 90 percent of the CPU. You identify the System process thread that causes the high CPU usage.

The thread has the start address ntkrnlpa.exe|ExpWorkerThread. You need to identify which functions the thread calls and how much CPU time each function uses. Which tool should you use?

- A. Kern rate
- B. Pstat
- C. Oslice
- D. Tlist

ANSWER:A

QUESTION NO:5

You have a computer that runs Windows Server 2008. You notice that the LSASS process uses a majority of the CPU time. You generate a complete memory dump file on the computer. You need to view the kernel-mode and user-mode stacks of all threads in the LSASS process. Which WinDbg command should you use?

- A. Nocks
- B. Iprocess
- C. (runaway
- D. Ivm

ANSWER:B

QUESTION NO:6

You are debugging a Windows device driver. The device driver has an unexpectedly long delay. 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
+0x016WaitType: 0

```

You need to identify 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. 5

ANSWER: B

QUESTION NO:7

You start a computer that runs Windows Vista. You attach a hardware device to the computer. You need to debug the creation of the functional device object (FDO) for the hardware device. Which routine should you debug?

- A. AddDevice()
- B. DriverEntry()
- C. DriverUnload()
- D. StartIo()

ANSWER:A

QUESTION NO:8

You create a new audio miniport driver. You need to test the driver by using the Driver Verifier tool. The tests must verify the following:

Memory overruns

Memory underruns

Memory that is accessed after it is freed

Which option of Driver Verifier should you use to test the driver?

- A. I/O verification
- B. Low resources simulation
- C. Pool tracking

D. Special pool

ANSWER:D

QUESTION NO:9

You are designing an application. The application fails because of an access violation. The access violation is caused by a heap corruption. You need to identify the cause of the heap corruption. Which tool should you use?

- A. Application Verifier
- B. Process Viewer
- C. Performance Monitor
- D. Task Manager

ANSWER:A

QUESTION NO:10

You plan to update a device driver on a Windows system. You download a copy of the device driver file from the Internet, but you are uncertain that the device driver is legitimate. You need to verify the device drivers digital signature. Which tool should you use?

- A. Certmgr.exe
- B. Certmgr.msc
- C. Makecert.exe
- D. Signtool.exe

ANSWER:D

QUESTION NO:11

You have an application named MyApp that fails intermittently and displays the following exception code: 0x00000005 The call stack shows that MyApp fails in various locations including ntdll.dll and MyApp.exe. The stack trace always includes the functions main and doRealWork. You review the source code for MyApp.exe and find the following code snippet:

```
#include <string.h>
#include <stdio.h>
extern void doRealWork(char*);
char* myfunc(char*);
void main(intargc,char*argv[])
{
char* szLocalBuffer;
```