



DIGITAL AND FORENSICS FUNDAMENTALS

KH4060CEM

Abstract

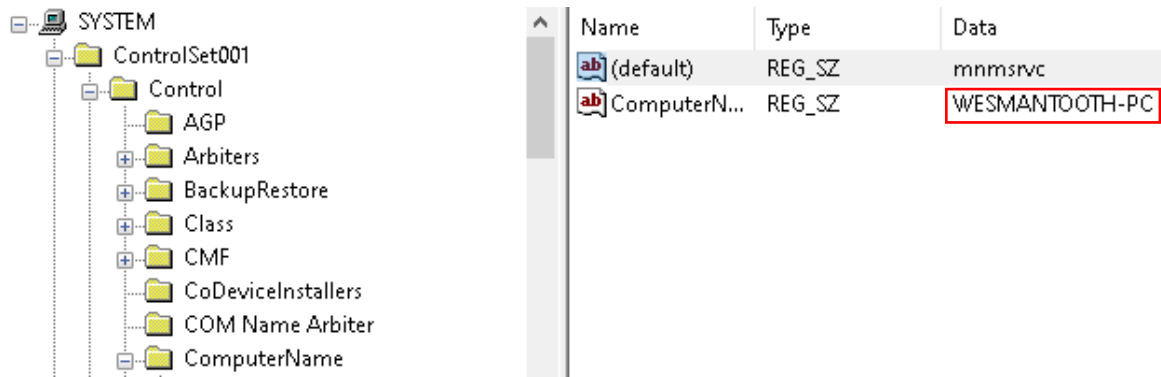
Answer all the questions

Ali M Abdelhamid

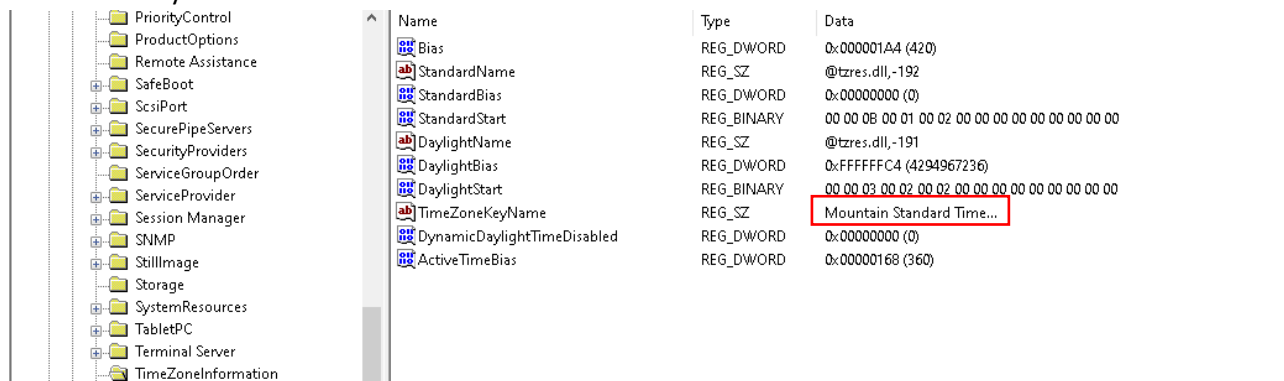
AA2100274

Digital and forensics fundamentals

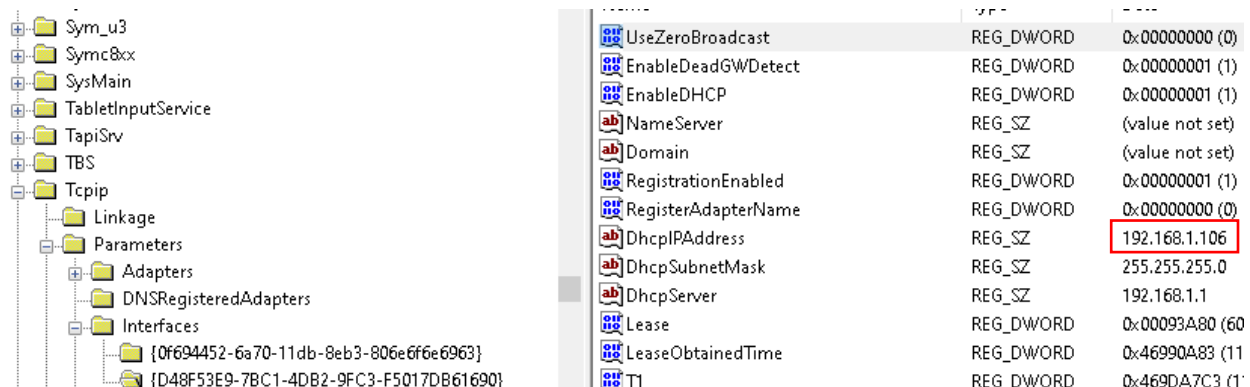
To begin with, the first question answer is “WESMANTOOTH-PC” that name was found by going to “ControlSet001” then to the file called “Control” then you’ll find a file name called “ComputerName” inside it you’ll find the data entry that contains the string called “WESMANTOOTH-PC” as seen here:



The second question's answer is “Mountain Standard Time” I accessed that by also going to the same file as before “ControlSet001” then “Control” then simply “TimeZoneInformation” and the key entry is “TimeZoneKeyName” as seen below:



The IP address for this machine is 192.168.1.106, finding this was a little bit more complicated, first “ControlSet001” then “Services” then the file called “Tcpip” then “Parameters” then “Interfaces” then the string entry called “{D48F53E9-7BC1-4DB2-9FC3-F5017DB6661690}” inside the DhcpIPAddress is found as found below:



The 4th answer is in the same file and the answer is “hsd1.co.comcast.net” also as shown below:

Name	Value
DhcpIPAddress	REG_SZ 192.168.1.106
DhcpSubnetMask	REG_SZ 255.255.255.0
DhcpServer	REG_SZ 192.168.1.1
Lease	REG_DWORD 0x00093A80 (604800)
LeaseObtainedTime	REG_DWORD 0x46990A83 (118443481)
T1	REG_DWORD 0x469DA7C3 (118473721)
T2	REG_DWORD 0x46A11DB3 (118496401)
LeaseTerminatesTime	REG_DWORD 0x46A24503 (118503961)
AddressType	REG_DWORD 0x00000000 (0)
IsServerNapAware	REG_DWORD 0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD 0x00000001 (1)
IPAutoconfigurationAddress	REG_SZ 0.0.0.0
DhcpInterfaceOptions	REG_BINARY 36 00 00 00 00 00 00 00
DhcpNameServer	REG_SZ 192.168.1.1
DhcpDefaultGateway	REG_MULTI_SZ 192.168.1.1
DhcpDomain	REG_SZ hsd1.co.comcast.net

The fifth question answer is “TREK TD2SMART G3M USB Device” “Sony Sony DSC USB Device” “SanDisk Cruzer Mini USB Device” and “Maxtor 6 B300R0 USB Device” there were also another device that got connected to the device called “Apple iPod USB Device” they are all located in “ControlSet001” then “Enum” then “USBSTOR” as shown below

- USBSTOR
 - Disk&Ven_Apple&Prod_iPod&Rev_1.62
 - 000A270014B302AB&0
 - Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_1000
 - 68&6b8c30&0&AA14012714842&0
 - AA14012714842&0
 - Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00
 - Disk&Ven_Maxtor_6&Prod_B300R0&Rev_BAH4
 - 8396
 - 8B76
 - Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.1
 - SNDK3066A40516400406&0
 - SNDK4DB2A41B47901706&0
 - Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.2
 - 20043513310C7A22D0C8&0
 - Disk&Ven_Sony&Prod_Sony_DSC&Rev_5.00
 - Disk&Ven_TREK&Prod_TD2SMART_G3&Rev_2.20
 - Disk&Ven_TREK&Prod_TD2SMART_G3M&Rev_2.40
 - Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_1100










The 6th question is what the last thing was mounted as the G drive, which is the Apple iPod device as shown here and it was last edited at 14/7/2007:

Last Written Time	7/14/2007 17:58:46 UTC
10 54 00 4F 00 52 00 23 00-44 00 69 00 73 00 6B 00	T-O-R-#-D-i-s-k
20 26 00 56 00 65 00 6E 00-5F 00 41 00 70 00 70 00	e-V-e-n-_-A-p-p-l-e-P-r-o-d-_-i-P-o-d-_-R-e-v-_-1-_-6-2-_-0-0
30 6C 00 65 00 26 00 50 00-72 00 6F 00 64 00 5F 00	0-A-2-7-0-0-1-4-
40 69 00 50 00 6F 00 64 00-26 00 52 00 65 00 76 00	B-3-0-2-A-B-6-0-
50 5F 00 31 00 2E 00 36 00-32 00 23 00 30 00 30 00	#-{-5-3-f-5-6-3-
60 30 00 41 00 32 00 37 00-30 00 30 00 31 00 34 00	0-7--b-b-f-f--
70 42 00 33 00 30 00 32 00-41 00 42 00 26 00 30 00	1-1-d-0--9-4-f-
80 23 00 7B 00 35 00 33 00-66 00 35 00 36 00 33 00	2--0-0-a-0-c-9-
90 30 00 37 00 2D 00 62 00-36 00 62 00 66 00 2D 00	1-e-f-b-8-b-}
a0 31 00 31 00 64 00 30 00-2D 00 39 00 34 00 66 00	
b0 32 00 2D 00 30 00 30 00-61 00 30 00 63 00 39 00	
c0 31 00 65 00 66 00 62 00-38 00 62 00 7D 00	

The 7th question is what the visited websites on internet explorer were, the answer is in the screen shot and I found them by opening the USER.DAT file and going to “Software” then “Microsoft” then simply the “Internet Explorer” key:

 url1	REG_SZ	http://www.flyertalk.com
 url2	REG_SZ	http://www.accessdata.com
 url3	REG_SZ	http://www.utah.com
 url4	REG_SZ	http://www.lasvegas.com
 url5	REG_SZ	http://www.newyork.com
 url6	REG_SZ	http://www.google.com/
 url7	REG_SZ	http://www.yahoo.com/
 url8	REG_SZ	http://www.nwa.com/
 url9	REG_SZ	http://www.usair.com/

The 8th question is asking about the path of PowerPoint the user opened. It's located in the “software” string then the “Microsoft” the follows “Office” then the version of office which is “10.0” then “PowerPoint” then recent file list. The path is “E:\KEITH\KEITH STUFF\Boot Camp 9-15\Day Mod-01- Introduction.ppt”:

 ney000ru	 File1	REG_SZ	E:\KEITH\KEITH STUFF\BootCamp 9-15\Day 1\Mod-01- Introduction.ppt
 MediaPlayer			
 MessengerService			
 Microsoft Management Console			
 MovieMaker			
 MS Design Tools			
 MSDAIPP			
 MSHandwritingTIP			
 Multimedia			
 NetDDE			
 NetShow			
 Ntbackup			
 Office			
 10.0			
 Access			
 Common			
 Excel			
 Outlook			
 PowerPoint			
 First Run			
 Options			
 Recent File List			

The 9th question is what the recent docs of the user and you can view that using RegRipper and ripping the USER.DAT evidence file. The files are as follows:

RecentDocs

**All values printed in MRUList\MRUListEx order.

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)

```
1 = Day 1
2 = Class Design.doc
9 = Explorer Exercise.doc
0 = Mod-01- Introduction.ppt
8 = FTK Exercise.doc
4 = MCI
3 = MCI.DOC
7 = MCIAIR.jpg
6 = Hertz Upgrade.jpg
5 = MCIHOTEL.jpg
```

The 10th question is the last commands entered by the user in order from recent to oldest, the answer is also found in RegRipper in the RunMRU section:

runmru v.20080324

(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)

MRUList = hbgfeacd

```
a regedit\1
b netstat\1
c command\1
d regedt32\1
e msconfig\1
f http://www.flyertalk.com\1
g http://www.htcia2003.com\1
h http://www.usair.com\1
```

The 11th question is what strings did the user search for in the system? The answer is also found in RegRipper in the ACMru section

acmru v.20080324

- Gets contents of user's ACMru key

ACMru - Search Assistant

Software\Microsoft\Search Assistant\ACMru

LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)

5603 [Thu Jan 1 00:00:00 1970 (UTC)]

000 -> module

5604 [Thu Jan 1 00:00:00 1970 (UTC)]

000 -> accessdata

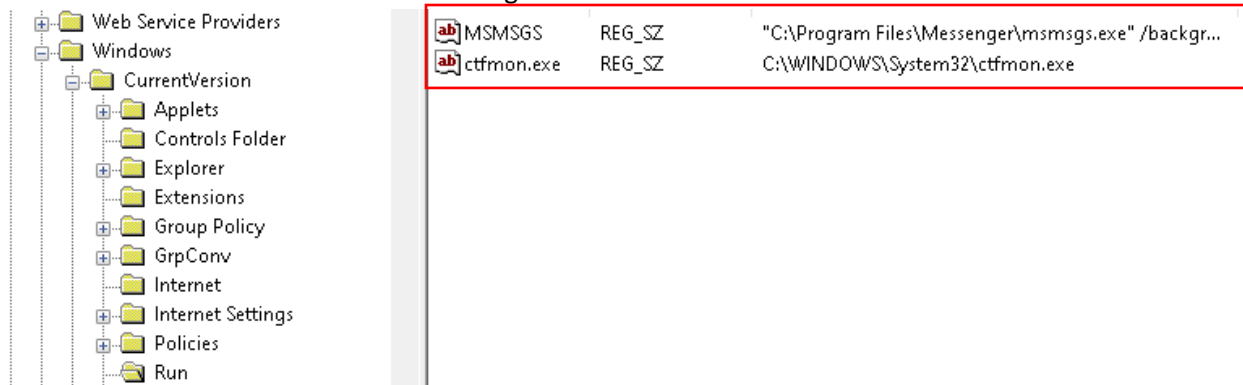
001 -> ftk

002 -> mod

003 -> lockhart

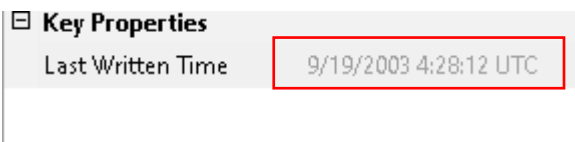
004 -> .doc

12th question answer is what programs run upon start-up of the computer? This time the answer is found in registry viewer in the “user.dat” evidence file, in the “software” file then “Microsoft” then “windows” and “current version” the string is called “Run”:



The 13th question is what .ink files would you expect to find on the computer. The .ink files you’d expect to find windows shortcut files, but these are just pointers that are built in windows to point to the original file.

The 14th question is when was the last time Netstat was run? The answer is found in registry viewer: netstat was last run 19/9/2003



the 15th question is how many times regedit was last run? I unfortunately could not find how many times as registry viewer did not preview this, but it was last run-on the 19th of September 2003 at 4:29:26 UTC:

