**Forensics CA 2:**

**RAM Capture Analysis**

**C22388703**

**James Lawlor**

Contents

[Question 1 3](#_Toc216022344)

[Question 2 4](#_Toc216022345)

[Question 3 5](#_Toc216022346)

[Question 4 6](#_Toc216022347)

[Question 5 7](#_Toc216022348)

[Question 6 8](#_Toc216022349)

[Question 7 9](#_Toc216022350)

[Question 8 10](#_Toc216022351)

[Question 9 11](#_Toc216022352)

[Question 10 12](#_Toc216022353)

[Question 11 13](#_Toc216022354)

[Question 12 14](#_Toc216022355)

[Question 13 15](#_Toc216022356)

# Question 1

**Question:** Using the pslist plugin identify the top 3 processes you would prioritize for deeper analysis. Justify your choices.

**Command:** ./vol -f xp-laptop-2005-06-25.img --profile=WinXPSP2x86 pslist

**Answer:** The processes I’d prioritize are as follows:

1. *firefox.exe* - Firefox is a web browser, and so looking further into it could provide new information about the subject’s internet activities.
2. *cmd.exe* - Command prompt allows for a lot of low-level system control, so it could be illuminating to potentially reveal more info such as what commands were run.
3. *dd.exe* - On a Windows system, this usually refers to a port of the Unix disk copy utility. It is also known for being used as part of certain malwares. It would be good to investigate further both to see if it is related to malicious activity, and to see what files were created or copied using it.

**Output:**

A screenshot of a computer program

AI-generated content may be incorrect.

# Question 2

**Question:** What processes have terminated in memory? What timestamps are associated with these exited processes?

**Command:** ./vol -f xp-laptop-2005-06-25.img --profile=WinXPSP2x86 pslist

**Answer:** Processes that have terminated are as follows:

|  |  |  |
| --- | --- | --- |
| Process Name | Process ID | Exit Stamp |
| PluckUpdater.exe | 3076 | 2005-06-25 16:51:30 UTC+000 |
| PluckUpdater.exe | 1916 | 2005-06-25 16:53:49 UTC+000 |
| PluckTray.exe | 3256 | 2005-06-25 16:54:28 UTC+000 |
| PluckTray.exe | 3100 | 2005-06-25 16:57:59 UTC+000 |

**Output:**

A screenshot of a computer program

AI-generated content may be incorrect.

# Question 3

**Question:** List all DLLs loaded by dd.exe. Are there any DLLs that look suspicious or unexpected for this type of process?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 dlllist -p 4012

**Answer:** The DLLs that seem most suspicious are the few that are stored outside of the normal system32 folder. This means the two DLLs that are stored in UnicodeRelease, which are “getopt.dll” and “MSVCR70.dll”.

**Output: A screenshot of a computer

AI-generated content may be incorrect.**

# Question 4

**Question:** What network activity patterns is associated with PID 1916?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 connscan | grep 1916

**Answer:** This process, which is PluckUpdater.exe, has a number of outgoing HTTP connections, and a single HTTPS connection. It is odd that an updater for a single application has connections made to so many different addresses, which is something that should be investigated further.

**Output:**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

# Question 5

**Question:** Is there any evidence of a connection to 192.168.1.100:443? If not, what HTTPS connection does appear in memory, and which process owns it?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 connscan | grep :443

**Answer:** No, there is no connection to the listed IP address in memory. There is however a single HTTPS connection, which belongs to PluckUpdater.exe, PID 4012, which was discussed in Question 4.

**Output:**

****

# Question 6

**Question:** Inspect the current users NTUSER.DAT to find what URLs were manually typed into the Internet Explorer address bar.

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -o 0xe1eff758 -K “Software\Microsoft\Internet Explorer\Typed URLs”

**Answer:** Only one URL is present, and seems to lead to microsoft.com. It also seems to feature a redirect, and to mention MSN Home.

**Output:**

**A computer screen with white text

AI-generated content may be incorrect.**

# Question 7

**Question:** List all autorun entries from HKLM...\Run.

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -K “Microsoft\\Windows\\CurrentVersion\\Run”

**Answer:** The command outputs a listing of all run keys.

**Output:**

**A computer screen shot of a program

AI-generated content may be incorrect.**

# Question 8

**Question:** Using the filescan plugin, list all gif files found in memory. What process id are they associated with? How many gifs are listing?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 filescan | grep gif

**Answer:** This command doesn’t directly list process IDs associated with the files, but we don’t need them. We can see from the directory that each gif is found in that they are, for the most part, related to either Internet Explorer (iexplore.exe, 2392) or Mozilla Firefox (firefox.exe, 2160). This goes the files in “Program Files\Mozilla Firefox\res” for Firefox, and those in “Documents and Settings\Sarah\Local Settings\Temporary Internet Files”. The two remaining gifs, “channelhead.gif” and “channeltail.gif” are unknown. There are 28 gifs in all.

**Output:**

**A screen shot of a computer screen

AI-generated content may be incorrect.**

# Question 9

**Question:** Inspect the files opened by dd.exe (PID 4012). Are there any unusual files or devices accessed? Is there any evidence available of the process activity?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 handles -p 4012 -t File

**Answer:** The listing here shows three files, all of them odd. Each of them is in a subdirectory called Device, and the second one appears to be a disk image, stored in a “HarddiskVolume1” folder. This could indicate that dd.exe was used to capture or copy a disk, and this image is the output.

**Output:**

**A screen shot of a computer

AI-generated content may be incorrect.**

# Question 10

**Question:** What IP addresses are linked with iexplore.exe?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 connscan | grep 2392

**Answer:** The listing here shows three IP addresses:

* 205.161.7.134
* 64.62.243.144
* 199.239.137.200

All of them were connected to via HTTP.

**Output:**

**A screen shot of a computer

AI-generated content may be incorrect.**

# Question 11

**Question:** List all the usernames of people on the system?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -K “SAM\Domains\Account\Users\Names”

**Answer:** The listing here shows 7 usernames:

* Administrator
* ASPNET
* Guest
* HelpAssistant
* phoenix
* Sarah
* SUPPORT\_388945a0

**Output:**

**A screenshot of a computer

AI-generated content may be incorrect.**

# Question 12

**Question:** What volume is in D Drive and what is the volume serial number?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -K “MountedDevices”

./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 symlinkscan | grep D:

./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -K “ControlSet001\Enum\USBSTOR”

**Answer:** The listing for the first command shows the data for several mounted drives, but it’s not hard to find the D: drive listing. Decoding the hexadecimal code under the listing reveals “\??\STORAGE#RemovableMedia#7&2930a404&0&RM#”. The output of the second command shows that D: is the DP(1)0-0+b drive discussed before. Looking at the two outputs, it is clear that D: is a removable drive, which makes it harder to capture information about it from RAM. I tried two more commands to attempt to retrieve information about removable drives from the USBSTOR hive, but neither drive I found there seemed to match. I was not able to retrieve the serial number in the end, and this task should be passed on to another analyst.

**Output:**

**A screenshot of a computer screen

AI-generated content may be incorrect.A computer screen shot of a program

AI-generated content may be incorrect.**

# Question 13

**Question:** What is the computers hostname?

**Command:** ./vol -f xp-laptop-2005-06-25.img –profile=WinXPSP2x86 printkey -K “ControlSet001\Control\ComputerName\ComputerName

**Answer:** At first, I tried the CurrentControlSet hive to look for this, but it didn’t have any meaningful data in it at all. ControlSet001 contained all the subkeys I expected of it, and produced output indicating that the hostname is “SPLATITUDE”.

**Output:**

**A computer screen with white text

AI-generated content may be incorrect.**