Case Name: Memory Analysis

Couse Name: IST402

Instructor: Robert Price

Date: 03/25/2025

Examiner Name: Jaspreet Singh

Table of Contents

List of Illustrative Materials

DumpIT

Armitage

Volatility

EXECUTIVE SUMMARY

Background

Throughout this investigation, the examiner primarily focuses on memory forensics and detecting signs of a compromised system through volatile data analysis. Since data stored in RAM is lost once a machine is powered down, the examiner captures a memory image beforehand using a forensic tool called DumpIt, which creates a full dump of the system's physical memory as a .raw image file.

To simulate an attack scenario, the examiner uses Armitage, a graphical interface for Metasploit, a widely used penetration testing framework. Armitage enables the examiner to identify and exploit system vulnerabilities through an accessible and visual interface.

After the simulated attack is carried out, the examiner applies Volatility, an open-source memory forensics tool written in Python, to analyze the captured RAM images. This tool extracts valuable data such as running processes, network connections, and system-level activity. By examining memory before and after the simulated attack, the examiner can identify signs of compromise and unauthorized access within the system.

Evidence

Description	File Name/Path	Source	Date/Time Collected	Examiner
Evidence	ram1.dd	Windows Server	03/30/2025 at 8:35 PM: Captured before the attack	Jaspreet Singh
Evidence	ram2.dd	Windows Server	04/30/2025 at 9:06 PM: Captured after the systems been compromised	Jaspreet Singh

COLLECTION AND ANALYSIS

Collection

The examiner began by first powering on the target Windows Server machine and launched basic applications such as Google Chrome to ensure that identifiable processes would be able to be present in memory. This was crucial for the examiner to do because it helps provide clear indicators when reviewing running processes later in the analysis phase of this forensic investigation.

Before any simulated attack was executed, the examiner used the forensic memory acquisition tool called DumpIt, to create a snapshot of the system's physical memory. Then once the tool was executed through the Windows command prompt line, and after confirming its operation, it was able to generate the examiner with a raw memory image. This initial dump of memory was saved and renamed to ram1.dd. Therefore, by capturing this image before the attack it was able to provide the examiner with a baseline reference of the system's normal and uncompromised state.

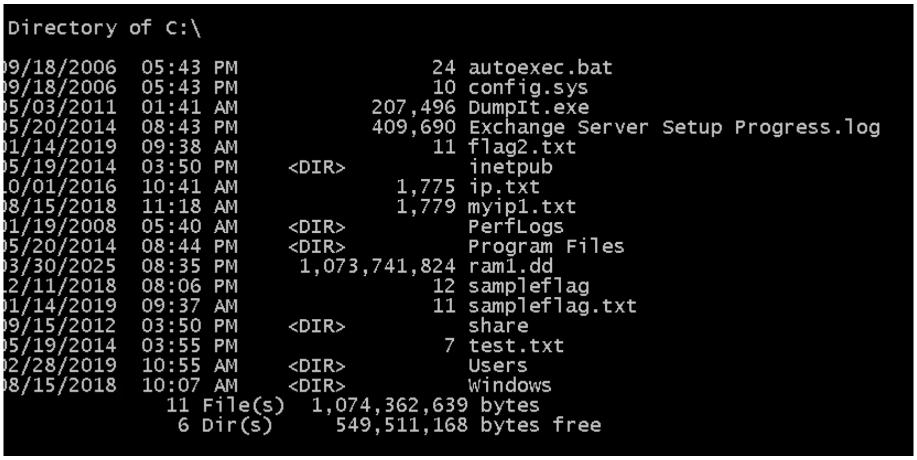
Once this memory image has been completed by using DumpIt, the examiner initialized a simulated an attack on the system using Armitage on a Kali Linux machine. Then after confirming that the system was successfully compromised, the examiner was able to return to the Windows Server machine to perform a second memory capture like before by using the forensic tool DumpIt. Then once this second image has been generated the examiner was able to rename this image to ram2.dd and this memory image represents how the system is after an attack has occurred.

Then the examiner was able to take both memory images, ram1.dd and ram2.dd, and transfer them to a secure location to perform further analysis. Having two separate captures of the system, one before and one after the attack, was crucial for the examiner to conduct a forensic review and compare them by highlighting any changes in running processes, network connections, or other memory-based artifacts introduced by the simulated attack. These memory images were then later analyzed by the examiner by using the open-source analysis tool Volatility, a memory forensics tool that enables in-depth examination of volatile data.

Analysis

DumpIt.exe directory

The examiner begins by opening the command prompt and running the following command c:\>DumpIt.exe to capture a complete snapshot of the system's physical memory (RAM). Once executed the examiner would view the directory and see that a new raw file was added which includes the whole snapshot of the system. The examiner then renames this file to ram1.dd by using the following command C:\> ren *.raw ram1.dd. Once this is completed the examiner can check the directory and verify that ram1.dd is present.

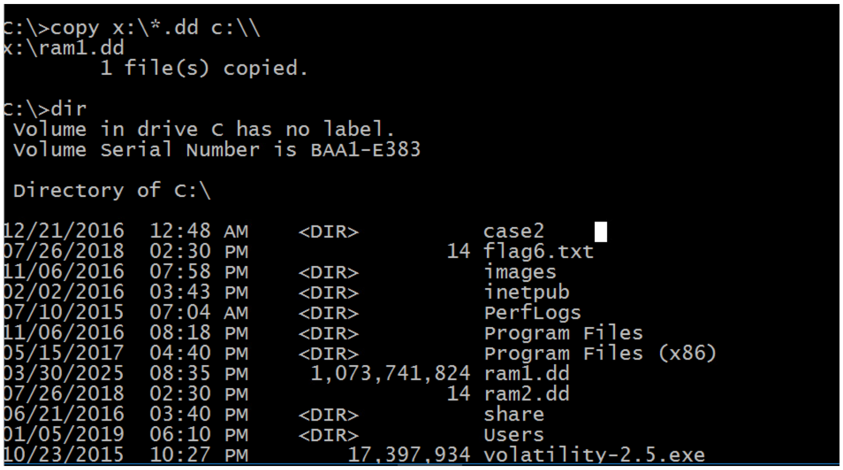


```
 Directory of C:\

9/18/2006  05:43 PM                24 autoexec.bat
9/18/2006  05:43 PM                10 config.sys
5/03/2011  01:41 AM           207,496 DumpIt.exe
5/20/2014  08:43 PM           409,690 Exchange Server Setup Progress.log
1/14/2019  09:38 AM                11 flag2.txt
5/19/2014  03:50 PM    <DIR>          inetpub
0/01/2016  10:41 AM             1,775 ip.txt
8/15/2018  11:18 AM             1,779 myip1.txt
1/19/2008  05:40 AM    <DIR>          PerfLogs
5/20/2014  08:44 PM    <DIR>          Program Files
3/30/2025  08:35 PM     1,073,741,824 ram1.dd
2/11/2018  08:06 PM                12 sampleflag
1/14/2019  09:37 AM                11 sampleflag.txt
9/15/2012  03:50 PM    <DIR>          share
5/19/2014  03:55 PM                 7 test.txt
2/28/2019  10:55 AM    <DIR>          Users
8/15/2018  10:07 AM    <DIR>          Windows
              11 File(s)  1,074,362,639 bytes
               6 Dir(s)     549,511,168 bytes free
```

Figure 1: DumpIt.exe ram1.dd created

Copying the Memory Dump

The examiner is creating a copy of the raw file ram1.dd by using the following command, copy x:\*.dd c:\. Then the examiner is able to view the directory again by using the command dir to verify that a copy has been created.

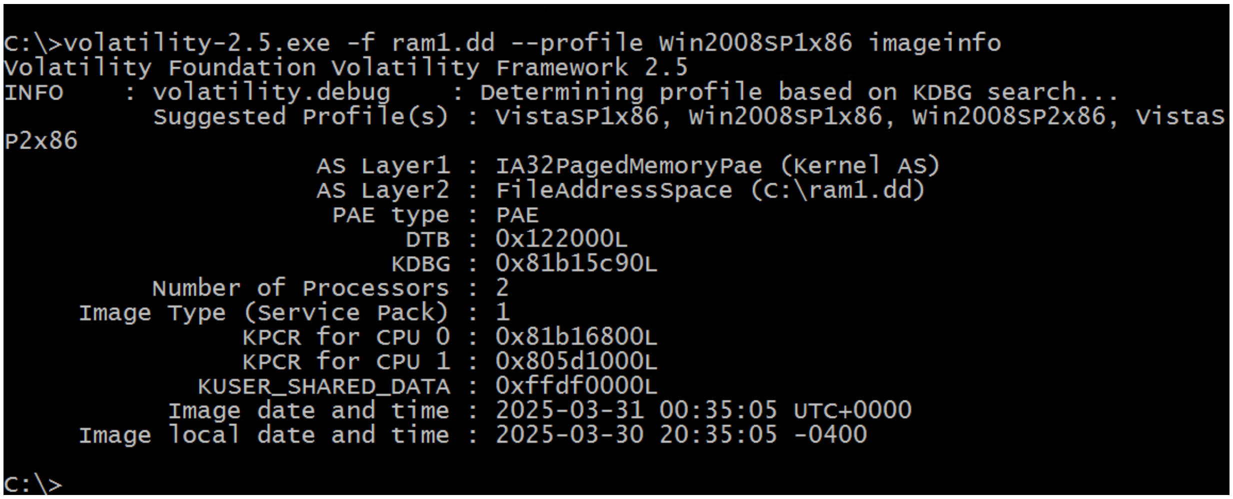


```
C:\>copy x:\*.dd c:\\
x:\ram1.dd
        1 file(s) copied.

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is BAA1-E383

 Directory of C:\

12/21/2016  12:48 AM    <DIR>          case2
07/26/2018  02:30 PM                14 flag6.txt
11/06/2016  07:58 PM    <DIR>          images
02/02/2016  03:43 PM    <DIR>          inetpub
07/10/2015  07:04 AM    <DIR>          PerfLogs
11/06/2016  08:18 PM    <DIR>          Program Files
05/15/2017  04:40 PM    <DIR>          Program Files (x86)
03/30/2025  08:35 PM     1,073,741,824 ram1.dd
07/26/2018  02:30 PM                14 ram2.dd
06/21/2016  03:40 PM    <DIR>          share
01/05/2019  06:10 PM    <DIR>          Users
10/23/2015  10:27 PM        17,397,934 volatility-2.5.exe
```

Figure 2: Copying ram1.dd

Volatility Image info

The examiner then runs a Volatility command on the ram1.dd file to gather information about the system's memory. The imageinfo command provides the examiner with details about the system profile, including the operating system version, architecture, and number of processors. This information is essential for selecting the correct profile for further analysis, such as identifying running processes and analyzing network connections.

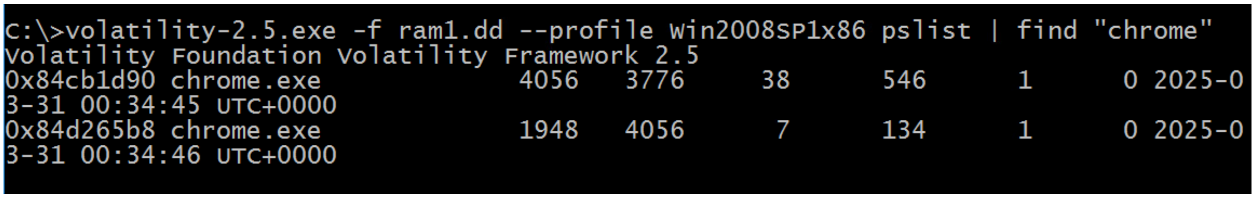


```
C:\>volatility-2.5.exe -f ram1.dd --profile Win2008SP1x86 imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
         Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaS
P2x86
                    AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                    AS Layer2 : FileAddressSpace (C:\ram1.dd)
                     PAE type : PAE
                          DTB : 0x122000L
                         KDBG : 0x81b15c90L
         Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x81b16800L
                KPCR for CPU 1 : 0x805d1000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2025-03-31 00:35:05 UTC+0000
     Image local date and time : 2025-03-30 20:35:05 -0400

C:\>
```

Figure 3: Volatility-2.5.exe

Finding "Chrome"

The examiner uses the Volatility command on the ram1.dd file to filter and identify instances where chrome.exe was running at the time of the memory capture. After executing the command, the examiner detects two active instances of chrome.exe in the memory image. This information establishes a baseline for comparison with the post-attack memory capture to identify any anomalies or unauthorized processes.



```
C:\>volatility-2.5.exe -f ram1.dd --profile Win2008SP1x86 pslist | find "chrome"
Volatility Foundation Volatility Framework 2.5
0x84cb1d90 chrome.exe              4056   3776     38      546      1      0 2025-0
3-31 00:34:45 UTC+0000
0x84d265b8 chrome.exe              1948   4056      7      134      1      0 2025-0
3-31 00:34:46 UTC+0000
```

Figure 4: Volatility-2.5.exe find "chrome"

Armitage

The examiner utilizes Armitage, a graphical user interface (GUI) front-end for Metasploit, which is designed to simplify and enhance the penetration testing process. In this investigation, the examiner uses Armitage to exploit a vulnerability in the target Windows system by selecting the SMB (Server Message Block) category and identifying a specific exploit named ms09_050_smb2_negotiate_func_index.

This exploit targets a vulnerability in the SMBv2 protocol, which allows remote attackers to gain elevated privileges on vulnerable Windows systems. After selecting the exploit, the examiner configures it by checking the option to "use a reverse connection," which establishes a connection back to the attacker's machine, enabling remote access and control over the compromised system. The examiner then launches the exploit, leading to the successful compromise of the target system with SYSTEM-level privileges.

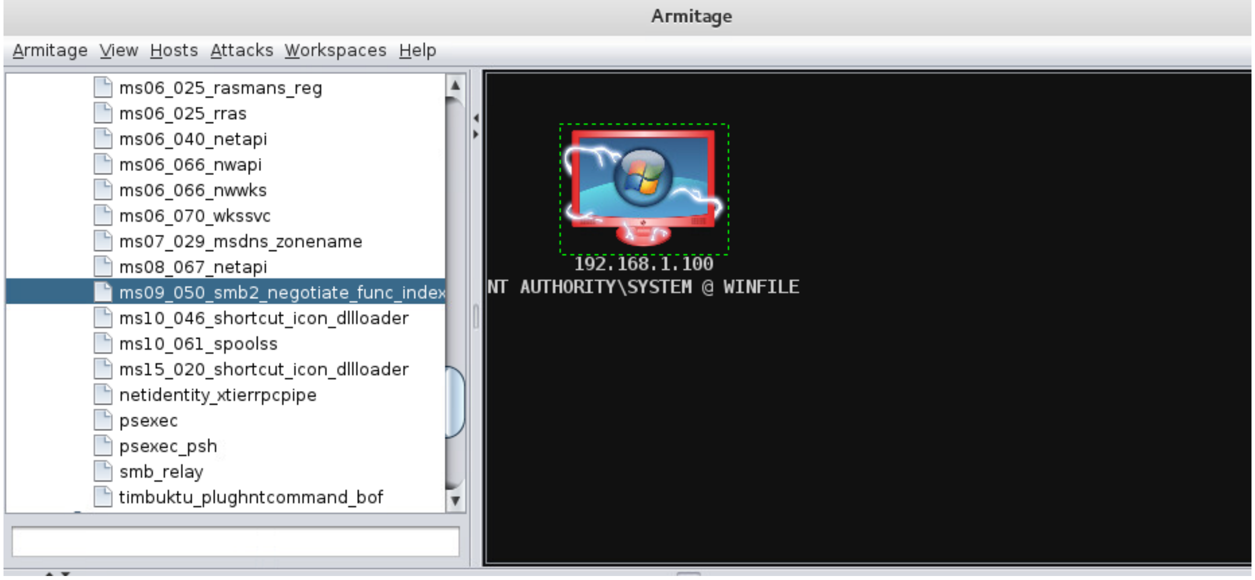
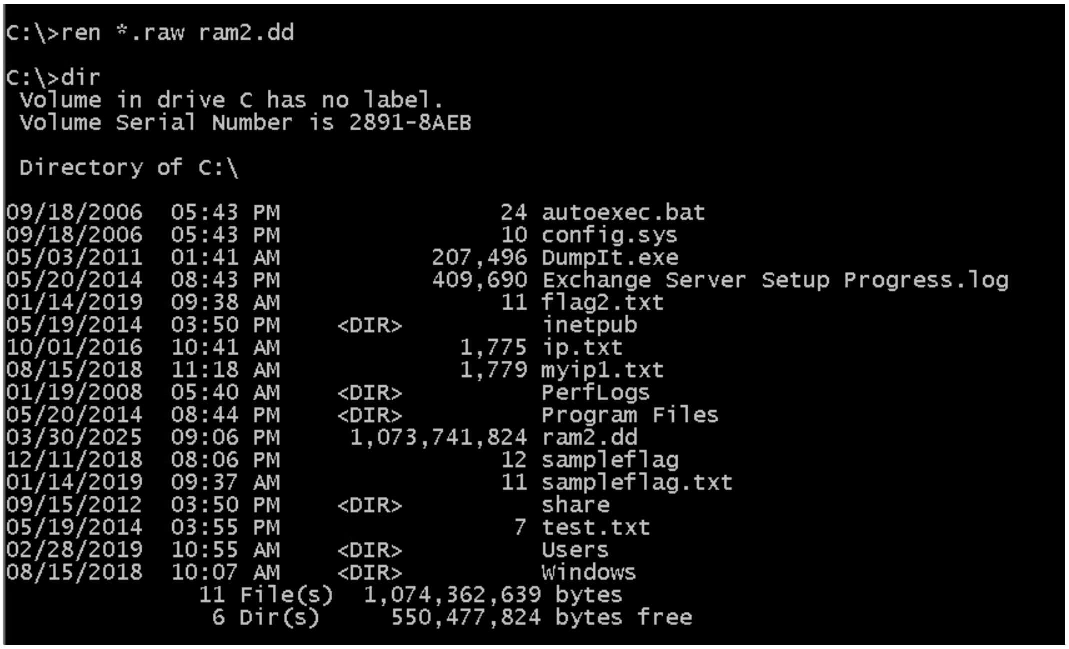


Figure 5: Using Armitage to exploit system

Deleting ram1.dd

The examiner begins by deleting the original ram1.dd file using the command del ram1.dd and verifies its removal by executing the dir command to list the contents of the directory. After ensuring that the original memory dump is deleted, the examiner runs DumpIt.exe again to capture a new snapshot of the system's RAM after the simulated attack. Once the new memory dump is generated, the examiner renames the file from its default .raw extension to ram2.dd using the command ren *.raw ram2.dd. Finally, the examiner performs another dir command to confirm that ram2.dd is successfully created and prepared for analysis.

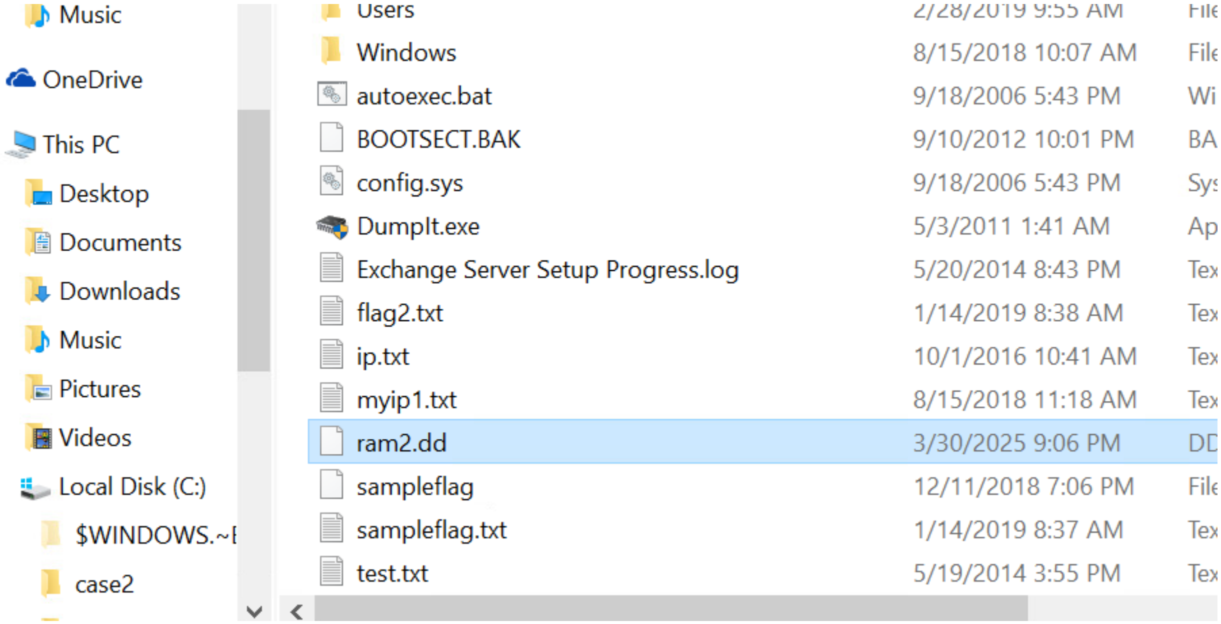


```
C:\>ren *.raw ram2.dd

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 2891-8AEB

 Directory of C:\

09/18/2006  05:43 PM                24 autoexec.bat
09/18/2006  05:43 PM                10 config.sys
05/03/2011  01:41 AM           207,496 DumpIt.exe
05/20/2014  08:43 PM           409,690 Exchange Server Setup Progress.log
01/14/2019  09:38 AM                11 flag2.txt
05/19/2014  03:50 PM    <DIR>          inetpub
10/01/2016  10:41 AM             1,775 ip.txt
08/15/2018  11:18 AM             1,779 myip1.txt
01/19/2008  05:40 AM    <DIR>          PerfLogs
05/20/2014  08:44 PM    <DIR>          Program Files
03/30/2025  09:06 PM     1,073,741,824 ram2.dd
12/11/2018  08:06 PM                12 sampleflag
01/14/2019  09:37 AM                11 sampleflag.txt
09/15/2012  03:50 PM    <DIR>          share
05/19/2014  03:55 PM                 7 test.txt
02/28/2019  10:55 AM    <DIR>          Users
08/15/2018  10:07 AM    <DIR>          Windows
              11 File(s)  1,074,362,639 bytes
               6 Dir(s)     550,477,824 bytes free
```

Figure 6: Creating ram2.dd file

Windows Key moving file

The examiner successfully transfers the ram2.dd file to the local C:\ drive after accessing the target system by using the Windows key and Run dialog. The examiner typed \\192.168.1.100\C$ to establish a connection to the target system's C:\ drive over the network and authenticated as an administrator to complete the transfer. This ensures that the post-attack memory dump is securely stored and ready for analysis.

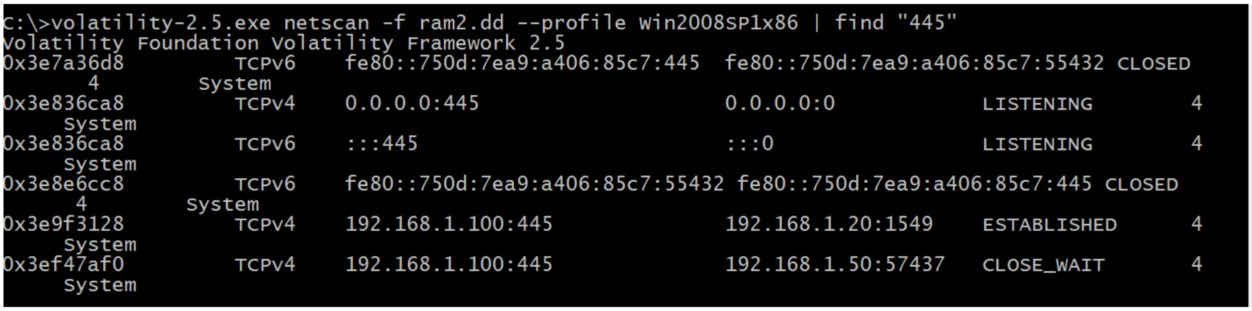


Users	2/28/2019 9:55 AM	File
Windows	8/15/2018 10:07 AM	File
autoexec.bat	9/18/2006 5:43 PM	Wi
BOOTSECT.BAK	9/10/2012 10:01 PM	BA
config.sys	9/18/2006 5:43 PM	Sys
DumpIt.exe	5/3/2011 1:41 AM	Ap
Exchange Server Setup Progress.log	5/20/2014 8:43 PM	Tex
flag2.txt	1/14/2019 8:38 AM	Tex
ip.txt	10/1/2016 10:41 AM	Tex
myip1.txt	8/15/2018 11:18 AM	Tex
ram2.dd	3/30/2025 9:06 PM	DD
sampleflag	12/11/2018 7:06 PM	File
sampleflag.txt	1/14/2019 8:37 AM	Tex
test.txt	5/19/2014 3:55 PM	Tex

Figure 7: Moving the ram2.dd file into the Local C: Drive

Volatility find “445”

In the command prompt, the examiner launches Volatility and uses the netscan command to analyze the ram2.dd memory dump for network activity. This command scans for open, closed, or listening network connections captured in the system’s memory. To narrow down the results, the examiner applies a filter to display only connections related to port 445, which is commonly associated with the SMB (Server Message Block) protocol.



```
C:\>volatility-2.5.exe netscan -f ram2.dd --profile Win2008SP1x86 | find "445"
Volatility Foundation Volatility Framework 2.5
0x3e7a36d8         TCPv6    fe80::750d:7ea9:a406:85c7:445  fe80::750d:7ea9:a406:85c7:55432 CLOSED
       4        System
0x3e836ca8         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4
     System
0x3e836ca8         TCPv6    :::445                         :::0                 LISTENING        4
     System
0x3e8e6cc8         TCPv6    fe80::750d:7ea9:a406:85c7:55432 fe80::750d:7ea9:a406:85c7:445 CLOSED
      4        System
0x3e9f3128         TCPv4    192.168.1.100:445              192.168.1.20:1549    ESTABLISHED      4
     System
0x3ef47af0         TCPv4    192.168.1.100:445              192.168.1.50:57437   CLOSE_WAIT       4
     System
```

Figure 8: Finding “445”

Conclusion

Overall, throughout this lab, the examiner was able to gain hands-on experience using multiple forensic tools to capture, analyze, and identify potential system compromises through memory forensics. For instance, the examiner used the following forensic memory tools, DumpIt, Armitage, and Volatility to simulate a real-world cyberattack, analyze the system’s activities, and identify post-attack artifacts that were preserved in memory dumps.

DumpIt

The examiner was able to utilize DumpIt to create a snapshot of the system’s volatile memory at two points during this lab. First was before the attack and after the attack was simulated. The first memory capture called ram1.dd provided the examiner with a baseline image of the system’s state prior to being exploited. Then after the attack was carried out by using Armitage, the examiner was able to create a second memory dump called ram2.dd which captured the systems memory after the attack had been carried out. Both these memory dumps were essential for conducting a comparative forensic analysis on the system and identifying any changes introduced by the simulated attack.

Armitage

The examiner utilized the graphical interface for Metasploit called Armitage, to simulate a successful cyberattack against the target windows system. This was completed by the examiner by selecting the ms09_050_smb2_negotiate_func_index exploit from the smb category. Then from there the examiner was able to compromise the system and gain system-level privileges. The use of the reverse connection allowed the examiner to maintain control over the system, providing the examiner with an opportunity to analyze the system after it has been exploited.

Volatility

Finally, the examiner analyzed the memory images using Volatility, an open-source memory forensics tool. The examiner applied the appropriate profile, Win2008SP1x86, to identify running processes using the pslist command and examine network connections through the netscan command. The analysis revealed multiple listening connections on port 445 and highlighted an established connection as well. These findings confirmed the presence of post-exploitation activity and provided evidence of potential system compromise.