# Memory Analysis Lab

In our last lab, we identified a hostname associated with a likely admin on a web server under investigation. The IP address of the web server was 85.242.72.23. Further analysis would have revealed the public IP associated with the incoming SSH connection on the box. We've been issued a warrant to search the residence associated with the IP address, and we found a device with a name matching the hostname in the authorized_keys file on the server.

We also obtained an encrypted SQLite database file, but we were unable to recover the password. This database likely contains information relevant to the case and recovering the password is now the primary objective of our investigation.

We were able to locate the host in the authorized_keys file and we have an image of the system's memory. In this lab, we will analyze the memory image for information related to the case.

## Lab

1. Boot up your lab host.
2. Launch PowerShell
3. Change directories into C:\Tools\Volatility

   ```
   cd C:\Tools\Volatility\
   ```

4. The memory image is stored in C:\Tools\Samples\physmem.raw. Before we can analyze it, we need to run **imageinfo** to determine the correct memory profile to use.

   ```
   PS C:\Tools\Volatility> .\volatility_2.6_win64_standalone.exe -f ..\Samples\physmem.raw imageinfo
   ```

   What is our preferred profile?

5. Let's check to see what network connections were active at the time of the image capture using **netscan**.

   ```
   PS C:\Tools\Volatility> .\volatility_2.6_win64_standalone.exe -f ..\Samples\physmem.raw --profile=Win7SP1x64 netscan
   ```

   What application was connected to the IP address of the web server? Putty.exe
   What was the associated remote port?

6. Now we have positive confirmation that this device was used to connect to the web server we investigated last time. Let's take a look at what processes were running at the time of the capture using **psxview**.

   ```
   PS C:\Tools\Volatility> .\volatility_2.6_win64_standalone.exe -f ..\Samples\physmem.raw --profile=Win7SP1x64 psxview
   ```

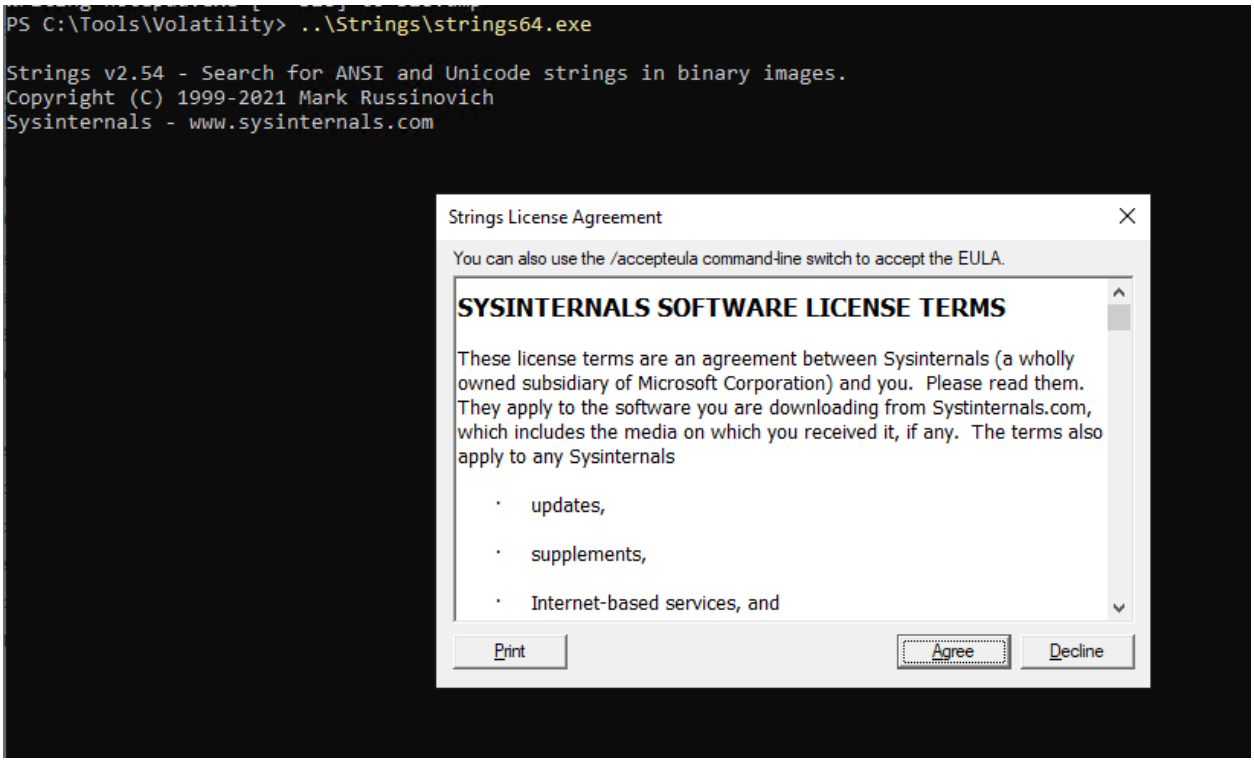
   Which processes are likely to contain user data?
   Are there any hidden processes?

7. Notepad is often a quick place to temporarily hold text, and it often contains sensitive data. Let's see what we can find in the process. Dump the process using the PID from the

previous command:

```
.\volatility_2.6_win64_standalone.exe -f ..\Samples\physmem.raw --profile=Win7SP1x64 memdump -p 328 --dump-dir .
```

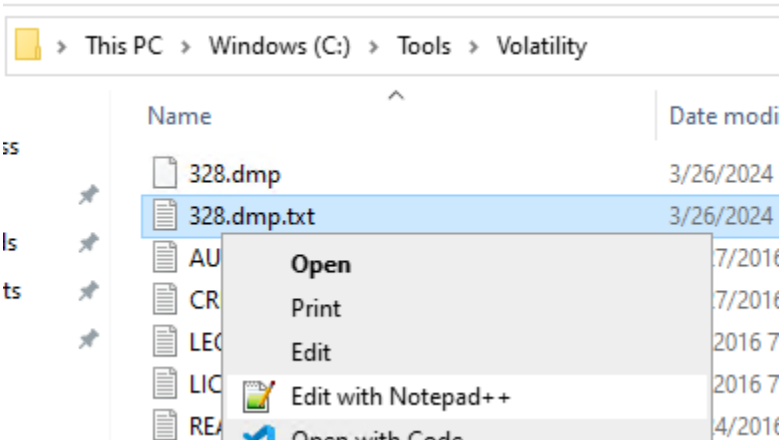
8. Now that we've dumped the contents of the process, let's use strings64.exe to look for strings contained within it. The first time you run strings64.exe, you will need to agree to the terms.



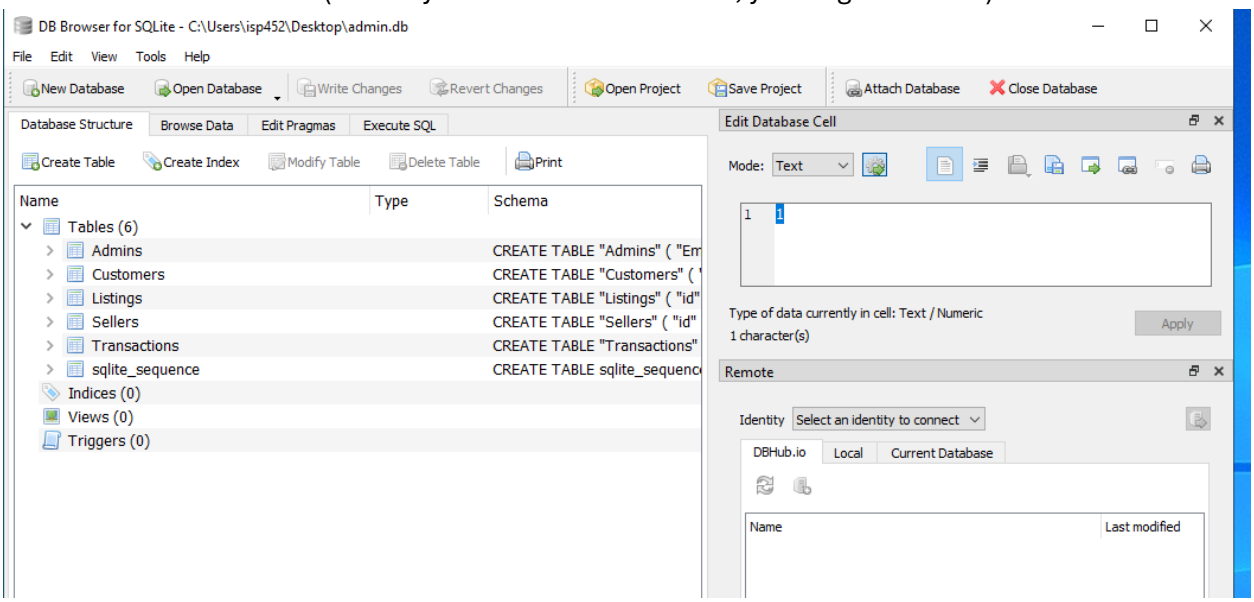

9. Now that we've agreed to the terms, let's run strings64.exe against the process dump and output the results into a new text file. This command may take a few minutes to complete.

```
PS C:\Tools\Volatility> ..\Strings\strings64.exe .\328.dmp > 328.dmp.txt
```

10. The resulting text file will be surprisingly large. Open it with notepad++. Don't use notepad as it doesn't handle large text files well.




11. Review the strings in the file. What is likely the password for the SQLite database file we recovered in the last lab? (Hint: If you've reached line 3000, you've gone too far).




12. Other than Benedict, what is the email address of the other admin on the site?

13. Bonus: what is the phone number of this user?