# CIS484-50-4218 Project 3

***Notes:***

* ***All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.***
* ***Provide all answers in UTC format.***
* ***Download the Project 3.7z archive from Blackboard under Projects\Project 3. Extract the contents of the downloaded archive using 7-Zip. Upon extraction, there should be four folders: Recycle Bin, Scheduled Tasks, Event Logs, and Prefetch Files.***

***Parse and Analyze $Recycle.Bin Files***

Parse the Recycle Bin $I files in the “Recycle Bin” folder using $I\_Parse and answer the following questions:

1. *How many different files were sent to this Recycle Bin, based on the available $I files?*
   * *6*
2. *What is the version of operating system from which these files were removed?*
   * *Windows 10*
3. *What date and time was “Luna Owl.jpg” sent to the Recycle Bin?*
   * *1/27/2017 17:35:49*
4. *What was the full path to “Pygmy Owl.jpg” before it was sent to the Recycle Bin?*
   * *C:\Users\Sarah M\Desktop\pets\Pygmy Owl.pdf*
5. *What is the name of the file that was sent to the Recycle Bin most recently?*
   * *01/31/2017 19:27:38*
6. *What is the file size in bytes of the largest file in this Recycle Bin?*
   * *593265*
7. *What is the animal pictured in “Next Pet.jpg”?*
   * *Sea Turtle*

***Analyze Scheduled Tasks***

Analyze the scheduled tasks in the “Scheduled Tasks” folder and answer the following questions:

1. *How often is GoogleUpdateTaskMachineCore scheduled to execute?* 
   * *Once a day*
2. *When is the “dkfo4f” scheduled task configured to execute?*
   * *When user WIN-LPUE2OJ805Q\Win7 logs in*
3. *When was the “dkfo4f” scheduled task created?*
   * *2013-06-20 11:28:50.5032431*
4. *What account created the “dkf04f” schedule task?*
   * *guest*
5. *What is the full path to the .exe that will launch when the “dff04f” scheduled task is triggered?*
   * *C:\Users\Win7\AppData\Local\Temp\dkfo4f.exe*

***Parse and Analyze Event Logs***

Parse the event logs in the “Event Logs” folder using Evtx Explorer (evtxcmd). Be sure to issue the sync command after downloading Evtx Explorer to download the latest maps (“evtxcmd.exe

–sync”). Analyze the output of Evtx Explorer using Timeline Explorer and answer the following questions:

1. *When was the most recent event record created?*
   * *9/19/2020 4:52:12 AM*

1. *How many Windows RDP logons are present in the event logs? To identify RDP logons, filter for Event ID 4624, Type 10 (i.e. “LogonType 10” in Payload Data2 column).*
   * *4*
2. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. Based on the map description, how many times was a computer account changed?*
   * *15*
3. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the name of the account that was deleted on 2020-09-18 01:05:16?*
   * *Mortysmith P492 in evtx*
4. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the name of the application that encountered an error on 2020-09-19?*
   * *Spoolsv.exe*
5. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. When is the last time the OS was shutdown?*
   * *9/18/2020 11:10:54 PM*
6. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. How many outgoing RDP connections are present in the event logs?*
   * *1*
7. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the target account associated with the most recent failed logon?*
   * *Administrator*
8. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the IP address of the remote host from which the RDP network connections were established on 2020-09-19?*
   * *194.61.24.102*
9. *Based on analysis of the event logs, on what day was VMWare Tools installed on the system?*
   * *9/17/2020 5:03:03 pm*
10. *Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the earliest creation date of the scheduled task called “\Microsoft\Windows\TPM\Tpm- Maintenance”?*
    * *9/17/2020 5:57:19 pm*
11. *What is the Security Identifier (SID) of the account that was logged in when the service “mszhao” was installed?*
    * *S-1-5-21-2232410529-1445159330-2725…*
12. *On what day was the account “summersmith” created?*
    * *9/18/2020 12:53:26 am*
13. *Based on analysis of the event logs, how many user accounts were created on this system and NOT deleted at a later date?*
    * *5*
14. *Based on analysis of the event logs, what is the name of the account associated with the security identifier (SID) “S-1-5-21-2232410529-1445159330-2725690660-502”?*
    * *Not an id with that SID. If it’s a typo, 500 then it is admin*
15. *Based on analysis of the event logs, what is the command that was executed 11 seconds after the first remote desktop services session logon on 2020-09-19? HINT: If two event records display the same created timestamp in Timeline Explorer, report the first of the two records (i.e. the record with the lowest “line number” value) for your answer.*
    * *3:22:38 and 22:37 cell C81484. The answer is in cell 81876. Finished execution of command, or C:\Windows\system32\vm3dservice.exe -u*

***Parse and Analyze Prefetch Files***

Parse the Prefetch files in the “Prefetch” folder using PECmd and answer the following questions, using both the verbose PECmd output as well as the PECmd timeline output.

1. *Based on analysis of the Prefetch files, what is the name of the program executed most recently?*
   * *SVCHOST.exe*
2. *Based on analysis of the Prefetch files, how many different program executions occurred on January 28, 2017?*
   * *9*
3. *Based on analysis of the Prefetch files, what is the most recent execution time of “\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSWOW64\CMD.EXE”?*
   * *2/2/2017 10:25:38 pm*
4. *Based on analysis of the Prefetch files, how many times was WMIC.exe executed?*
   * *10*
5. *What is the volume serial number of the volume from which WMIC.exe was executed?*
   * *14412537*
6. *Based on analysis of the Prefetch files, what is the number of locations from which CMD.exe has been executed?*
   * *2*
7. *What is the operating system version associated with the parsed Prefetch files?*
   * *Windows 10*
8. *Based on analysis of the Prefetch files, what is the name of the program that has been executed 62 times from a single location?*
   * *Chrome*
9. *Based on analysis of the Prefetch files, what is the second-most recent execution time of “IASTORICON.EXE”?*
   * *2/1/2017 7:08:54 PM*