CIS 484-78-4212

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? 01/27/2017 17:35:49 UTC
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.jpg
5) What is the name of the file that was sent to the Recycle Bin most recently? C:\Users\Sarah M\Desktop\Next pet.jpg
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"? Turtle

Analyze Scheduled Tasks

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

8) How often is GoogleUpdateTaskMachineCore scheduled to execute? Daily
9) When is the "dkfo4f" scheduled task configured to execute? When user WIN-LPUE2OJ805Q\Win7 Logs on
10) When was the "dkfo4f" scheduled task created? 2013-06-20T11:28:50
11) What account created the "dkf04f" schedule task? WIN-LPUE2OJ805Q\Guest
12) 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:

13) When was the most recent event record created? 9/19/20 4:52 AM

14) 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
15) 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
16) 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? Morty Smith
17) 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? C:\Windows\System32\spoolsv.exe
18) Group the Evtx Explorer output by “Map Description” in Timeline Explorer. When is the last time the OS was shutdown? 2020-09-18 23:10:53
19) Group the Evtx Explorer output by “Map Description” in Timeline Explorer. How many outgoing RDP connections are present in the event logs? 1
20) Group the Evtx Explorer output by “Map Description” in Timeline Explorer. What is the target account associated with the most recent failed logon? Administrator
21) 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
22) Based on analysis of the event logs, on what day was VMWare Tools installed on the system? 2020-09-17 17:03:03
23) 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”? 2020-09-17 17:57:18
24) What is the Security Identifier (SID) of the account that was logged in when the service “mszhao” was installed? Account: LocalSystem, SID: S-1-5-21-2232410529-1445159330-2725690660-500
25) On what day was the account “summersmith” created? 2020-09-18 00:53:25
26) Based on analysis of the event logs, how many user accounts were created on this system and NOT deleted at a later date? 7
27) 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”? krbtgt
28) 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. "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.

29) Based on analysis of the Prefetch files, what is the name of the program executed most recently? SVCHOST.EXE
30) Based on analysis of the Prefetch files, how many different program executions occurred on January 28, 2017? 15

31) Based on analysis of the Prefetch files, what is the most recent execution time of "\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSWOW64\CMD.EXE"? 2017-02-02 22:25:37

32) Based on analysis of the Prefetch files, how many times was WMIC.exe executed? 10

33) What is the volume serial number of the volume from which WMIC.exe was executed? 14412537

34) Based on analysis of the Prefetch files, what is the number of locations from which CMD.exe has been executed? 2

35) What is the operating system version associated with the parsed Prefetch files? Windows 10

36) 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.EXE

37) Based on analysis of the Prefetch files, what is the second-most recent execution time of "IASTORICON.EXE"? 2017-02-01 19:08:54