GENERAL INFORMATION

Mission Name

ForensicsTest

History Background

In the previous mission, ETHAN is arrested by Claire and Tarain. Claire and Ethan are going to work together to catch the SHAX hackers and both must be tested on their skills.

Technical High-Level Overview

Player must put in practice his knowledge about investigation event logs. The goal of this mission is to identify which event record id was deleted on Phaldra´s Computer.

Short Mission Description

You´re going to be tested to ensure your forensic knowledge is up to date. Please identify which event id record was deleted. Keep in mind, your goal, implies to analyse every event log file.

Mission Description

Player must put in practice his knowledge about locating tools to delete Windows events. You´re going to be tested to ensure that your knowledge is up to date. Please identify which event id record was deleted. Keep in mind, your goal, implies to analyse every event log file on Phaldras´s computer in 2049 when Phaldra tried to hide his footprints.

Location

SYLVARCON | EBAND DEPARTMENT - RECON HQ

Tools

- FTK Imager
- Event Log Explorer - https://eventlogxp.com/

Questions

Which event id was deleted?

- 7045

Which tool was used to delete events?

- DeleteRecordofFileEx.exe

Hints

1. Locate any tool to deleted eventlogs on Desktop folder.
2. System.evtx was tampered.
3. Compare System.evtx located on Phaldras Desktop and System.evtx on legit folder

Write Up

First of all, player should mount evidence provided to extract event logs, using FTK imager:

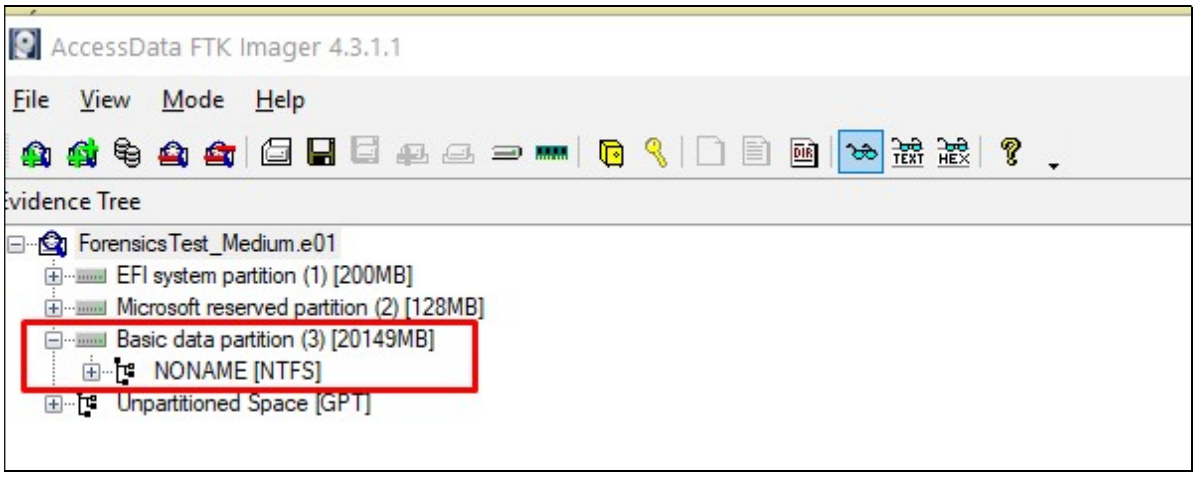


Figure 1

Later, player must extract all event logs located at: C:\Windows\System32\winevt\Logs:

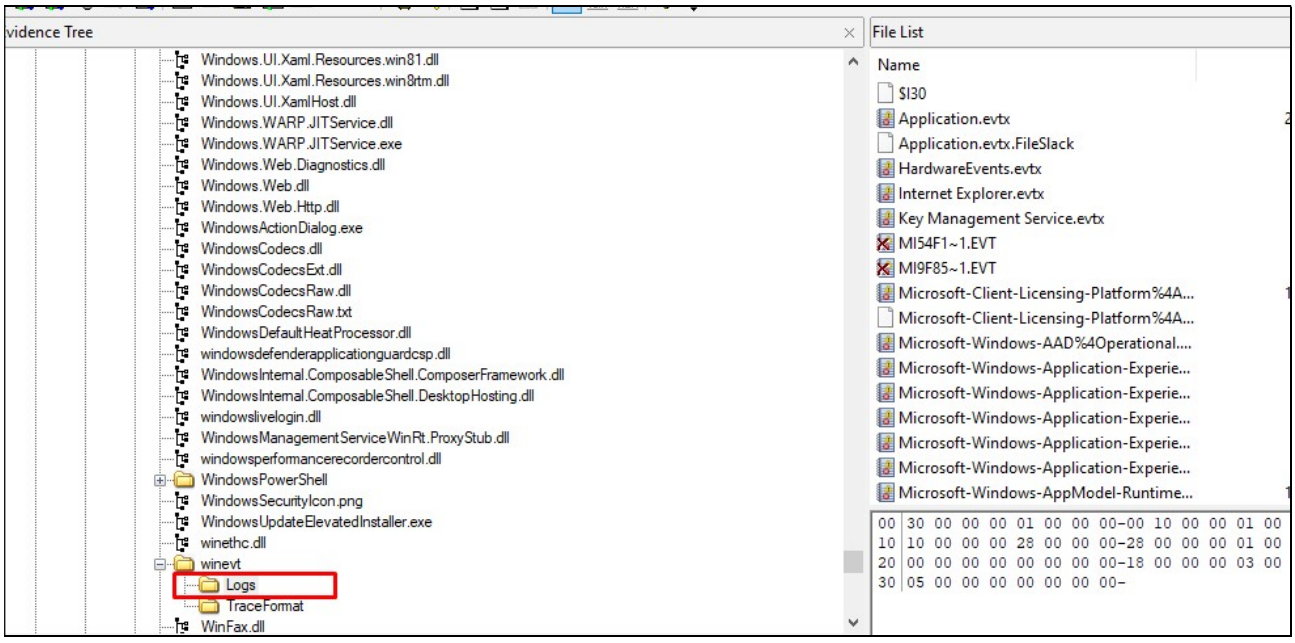
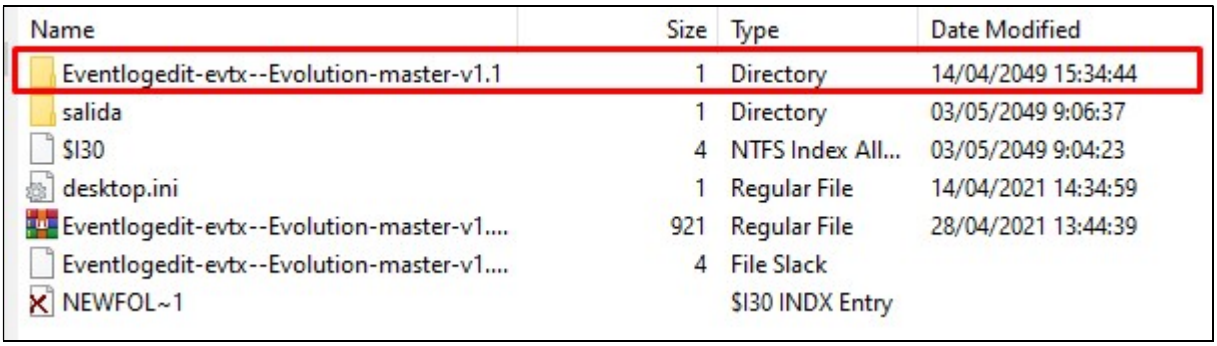


Figure 2

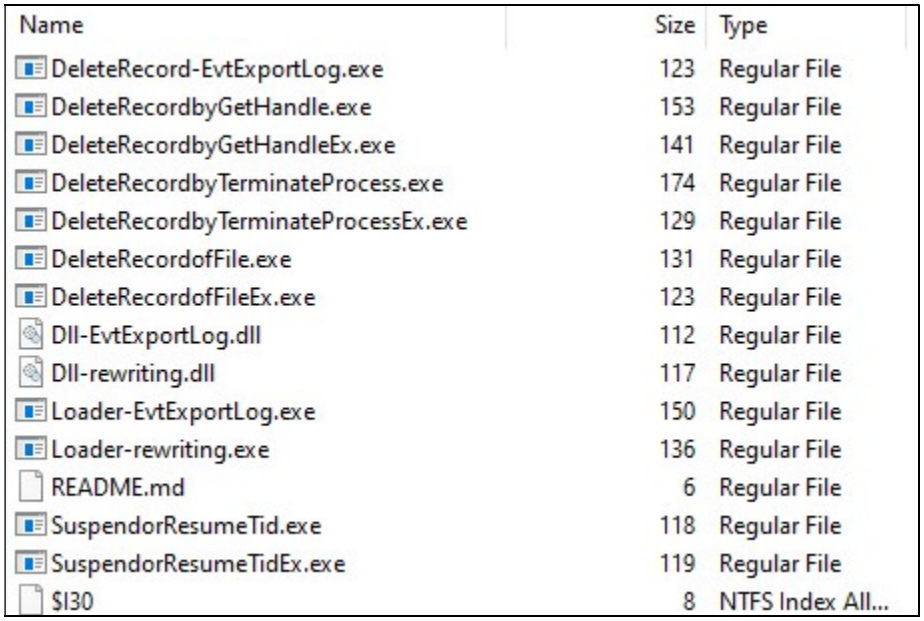
Player must analyse all events log to identify which event log record id was deleted. The clue is located on several folders on Phaldra´s Desktop:



Name	Size	Type	Date Modified
Eventlogedit-evtx--Evolution-master-v1.1	1	Directory	14/04/2049 15:34:44
salida	1	Directory	03/05/2049 9:06:37
$I30	4	NTFS Index All...	03/05/2049 9:04:23
desktop.ini	1	Regular File	14/04/2021 14:34:59
Eventlogedit-evtx--Evolution-master-v1....	921	Regular File	28/04/2021 13:44:39
Eventlogedit-evtx--Evolution-master-v1....	4	File Slack	
NEWFOL~1		$I30 INDX Entry	

Figure 3

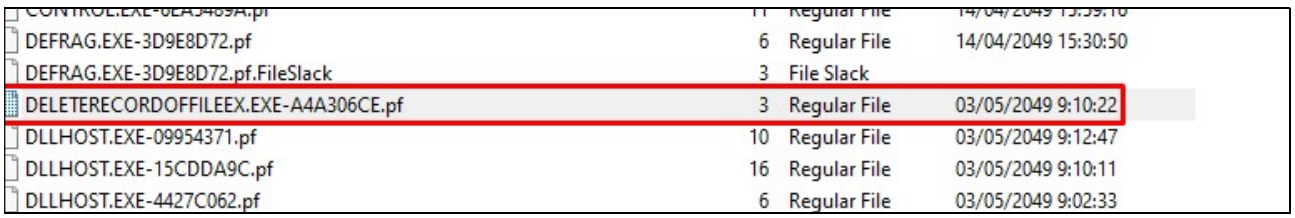
The first clue would be to identify this folder, it seems to be, binaries to deleted event logs:



Name	Size	Type
DeleteRecord-EvtExportLog.exe	123	Regular File
DeleteRecordbyGetHandle.exe	153	Regular File
DeleteRecordbyGetHandleEx.exe	141	Regular File
DeleteRecordbyTerminateProcess.exe	174	Regular File
DeleteRecordbyTerminateProcessEx.exe	129	Regular File
DeleteRecordofFile.exe	131	Regular File
DeleteRecordofFileEx.exe	123	Regular File
Dll-EvtExportLog.dll	112	Regular File
Dll-rewriting.dll	117	Regular File
Loader-EvtExportLog.exe	150	Regular File
Loader-rewriting.exe	136	Regular File
README.md	6	Regular File
SuspendorResumeTid.exe	118	Regular File
SuspendorResumeTidEx.exe	119	Regular File
$I30	8	NTFS Index All...

Figure 4

At this point, player might consider looking at the security events to identify de execution of this binaries or prefetch files. For this challenge, security events (Security.evtx) were deleted, so the last evidence would be to check prefetch:



DEFRAG.EXE-3D9E8D72.pf	6	Regular File	14/04/2049 15:30:50
DEFRAG.EXE-3D9E8D72.pf.FileSlack	3	File Slack	
DELETERECORDOFFILEEX.EXE-A4A306CE.pf	3	Regular File	03/05/2049 9:10:22
DLLHOST.EXE-09954371.pf	10	Regular File	03/05/2049 9:12:47
DLLHOST.EXE-15CDDA9C.pf	16	Regular File	03/05/2049 9:10:11
DLLHOST.EXE-4427C062.pf	6	Regular File	03/05/2049 9:02:33

Figure 5

It´s a shame, Prefetch doesn´t show which command was launched. Other clue to investigate would be on Phaldra´s Desktop:

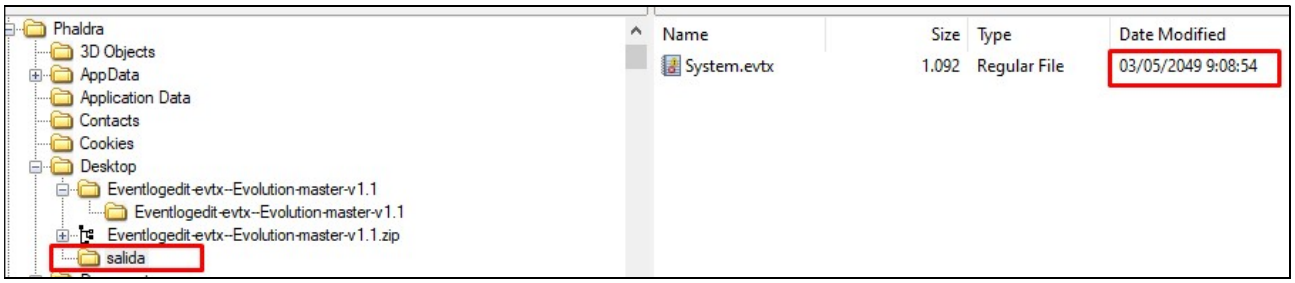


Figure 6

Date Modified of Security.evtx is close to Prefetch file, speaking in terms of dates. At his point, player having identified this clue, their goal would be analyse System.evtx on Phaldra´s Desktop and Security.evtx on the legit folder.

Legit Security Evtx filtered by 7045 event id:

Type	Date	Time	Event	Source	Categ
Information	14/04/2049	17:54:03	7045	Service Control Manag	None
Information	14/04/2021	17:15:39	7045	Service Control Manag	None
Information	14/04/2021	17:15:25	7045	Service Control Manag	None
Information	14/04/2021	17:15:25	7045	Service Control Manag	None
Information	06/04/2021	21:03:27	7045	Service Control Manag	None
Information	06/04/2021	21:03:27	7045	Service Control Manag	None
Information	06/04/2021	20:04:00	7045	Service Control Manag	None
Information	06/04/2021	17:55:34	7045	Service Control Manag	None
Information	06/04/2021	17:55:30	7045	Service Control Manag	None
Information	06/04/2021	17:55:29	7045	Service Control Manag	None

Figure 7

Phaldra Security Evtx filtered by event id 7045:

Filtered: showing 25 of 1619 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	03/05/2049	11:02:54	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	14/04/2049	17:54:03	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	14/04/2021	17:15:39	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	14/04/2021	17:15:25	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	14/04/2021	17:15:25	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	06/04/2021	21:03:27	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	06/04/2021	21:03:27	7045	Service Control Manag	None	\S-1-5-21-727859889-85	DESKTOP-B7AUQEA
Information	06/04/2021	20:04:00	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:34	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:30	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:29	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:29	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:29	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:29	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:23	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA
Information	06/04/2021	17:55:23	7045	Service Control Manag	None	\SYSTEM	DESKTOP-B7AUQEA

Figure 8

Phaldra deleted a event record id, in this case, an event id 7045:

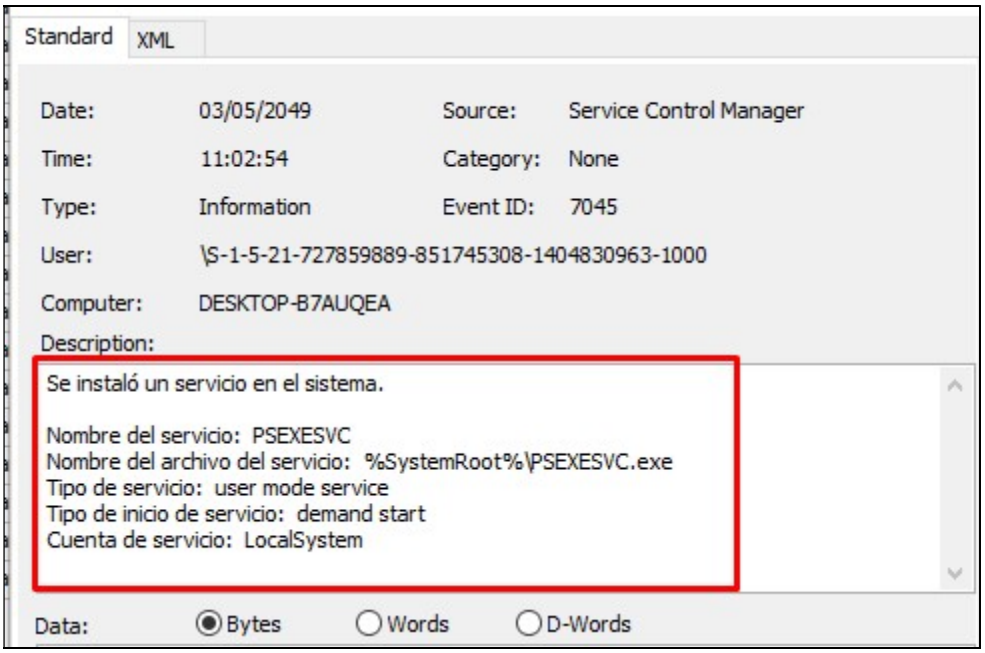


Figure 9

With event record id:

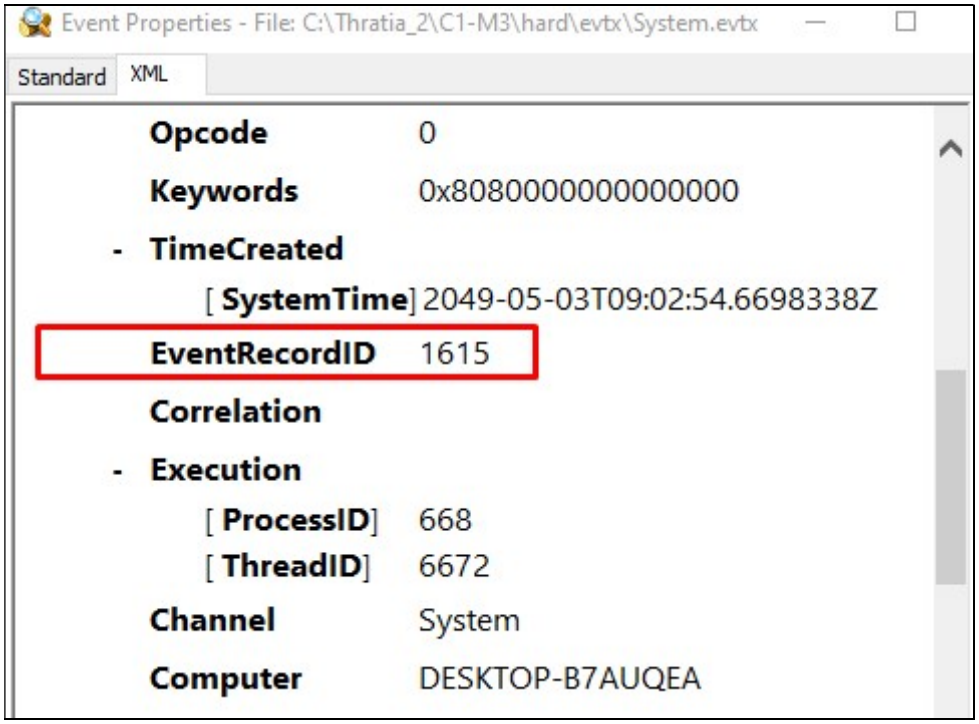


Figure 10

Flag Information

flag{1615}