AMcache

بسم الله الرحمن الرحيم

What Is amcache

هو يعتبر artifact موجود في ويندوز يساعدنا بالتحليل الجنائي وش المعلومات اللي يحتوي عليها؟

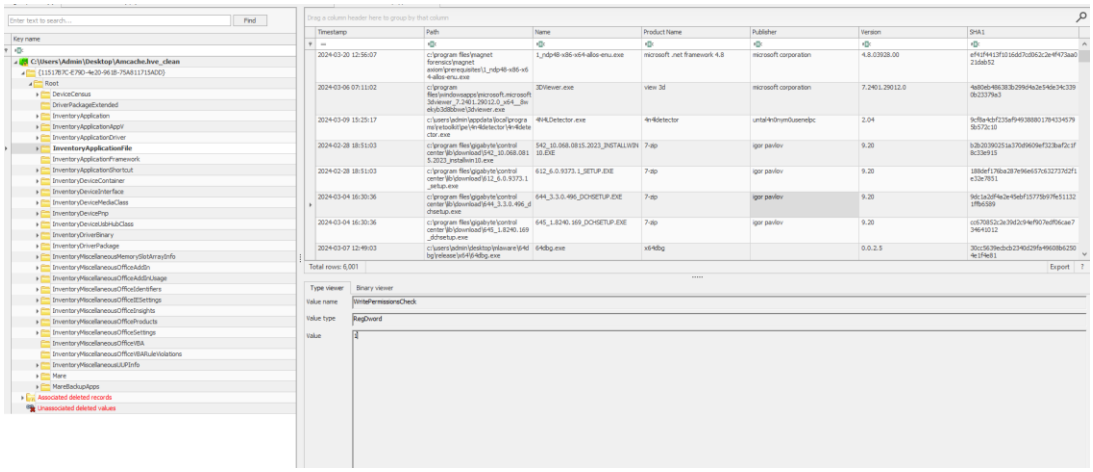
every executable runs	يسجل كل برنامج اشتغل
full path information	المسار الكامل للبرنامج
SHA1 hash	الهاش حق البرنامج
last time executed	اخر مرة اشتغل البرنامج
Hardware information	معلومات عن الأجهزة
drivers information	معلومات عن الدريفرز بالجهاز و الهاش حقها

How to get Amcache

المسار راح يكون

```
C:\Windows\Appcompat\Programs\Amcache.hve
```

و راح نستخدم registry explorer عشان نفتح الملف



هذي نظرة عامة عن البرامج اللي اشتغلت ممكن أحد افضل الاشياء اللي تسويها انك تاخذ كل ال SHA1 و تبحث عنها في virus total باستخدام تولز لأنها بتسرع عليك التحليل لو كان الهاش معروف

	center\lib\mbstorage\msio32.sys					
2024-02-28 18:51:03	c:\program files\gigabyte\control center\lib\mbstorage\msio64.sys	MsIo64.sys	msio64 driver version 1.3	micsys technology co., ltd	1.3 x64 built by: winddk	1de9f2 3538ce
2024-09-10 10:55:45	c:\windows\system32\drivers\nm3.sys	nm3.sys	microsoft network monitor 3 driver	microsoft corporation	3.4.2350.0	63efc0 35cd3c
2024-05-28 16:36:38	c:\program files\npcap\npcap.sys	npcap.sys	npcap	insecure.com llc.	1.78	ca5a73 38c36a

ويعطيني بعد ال sys وهي الdrivers اللي تشتغل في الجهاز حقي ف ممكن يساعدني شوي في تحليل اذا كان فيه rootkit بالجهاز او لا

DELL E2420HS				display.monitor	{b492fd48-84ca-f563-786a-9a41 cb9c}
Microsoft Software Printer Driver	OneNote for Windows 10			printfax.printer.virtual	{b29d9289-6cd5-fa63-e747-7cdb ad72}
B760 GAMING X	KIRA-PC	Default string	Gigabyte Technology Co., Ltd.	computer.desktop	
SteelSeries Apex 3 TKL				input.keyboard	{b534f2c2-77e3-568c-e32e-f431 e1ef}
VLI Product String				storage	{961c5416-a254-f1fb-c029-3b35 5ba}

ممكن بعد يعطيني تفاصيل عن الاجهزة اللي انشبكت بالجهاز مثل شاشات او كيبورد او ماوس

Timestamp	Model	Manufacturer	Description	Install Date
=	abc	abc nv	abc	abc
2025-03-22 12:12:43	HID-Compliant Mouse	Hanvon Ugee Technology	HID-Compliant Mouse	02-13-2025
2025-03-22 12:12:43	NVIDIA GeForce RTX 4070 SUPER	NVIDIA	NVIDIA GeForce RTX 4070 SUPER	03-08-2024
2025-03-22 12:12:43	Standard NVM Express Controller	Standard NVM Express Controller	Standard NVM Express Controller	02-28-2024
2025-03-22 12:12:43	Standard NVM Express Controller	Standard NVM Express Controller	Standard NVM Express Controller	09-18-2024
2025-03-22 12:12:43	OpenVPN Data Channel Offload	OpenVPN, Inc	OpenVPN Data Channel Offload	12-28-2024
2025-03-22 12:12:43	NvModuleTracker Device	NVIDIA	NvModuleTracker Device	02-28-2025
2025-03-22 12:12:43	NVVHCI Enumerator	NVIDIA	NVVHCI Enumerator	02-28-2025

هنا مثال عطاني نوع كرت الشاشة وممكن يعطيك المعالج و الرام