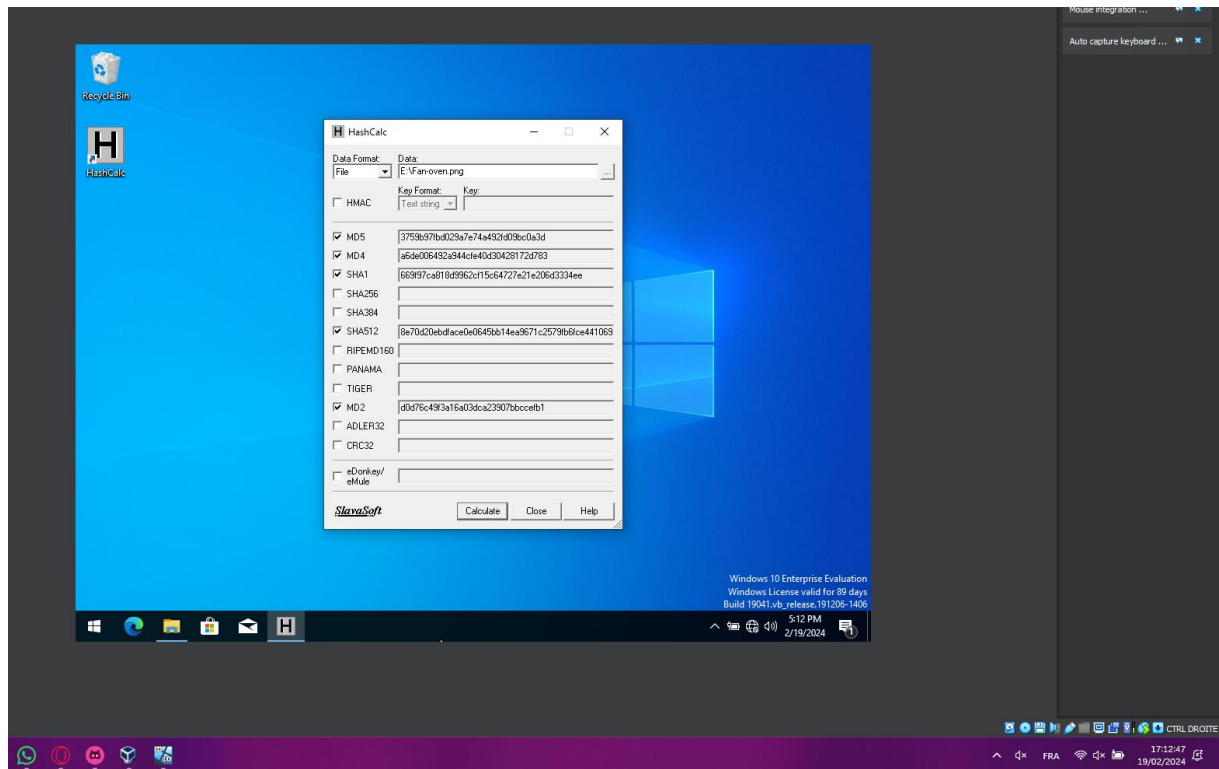


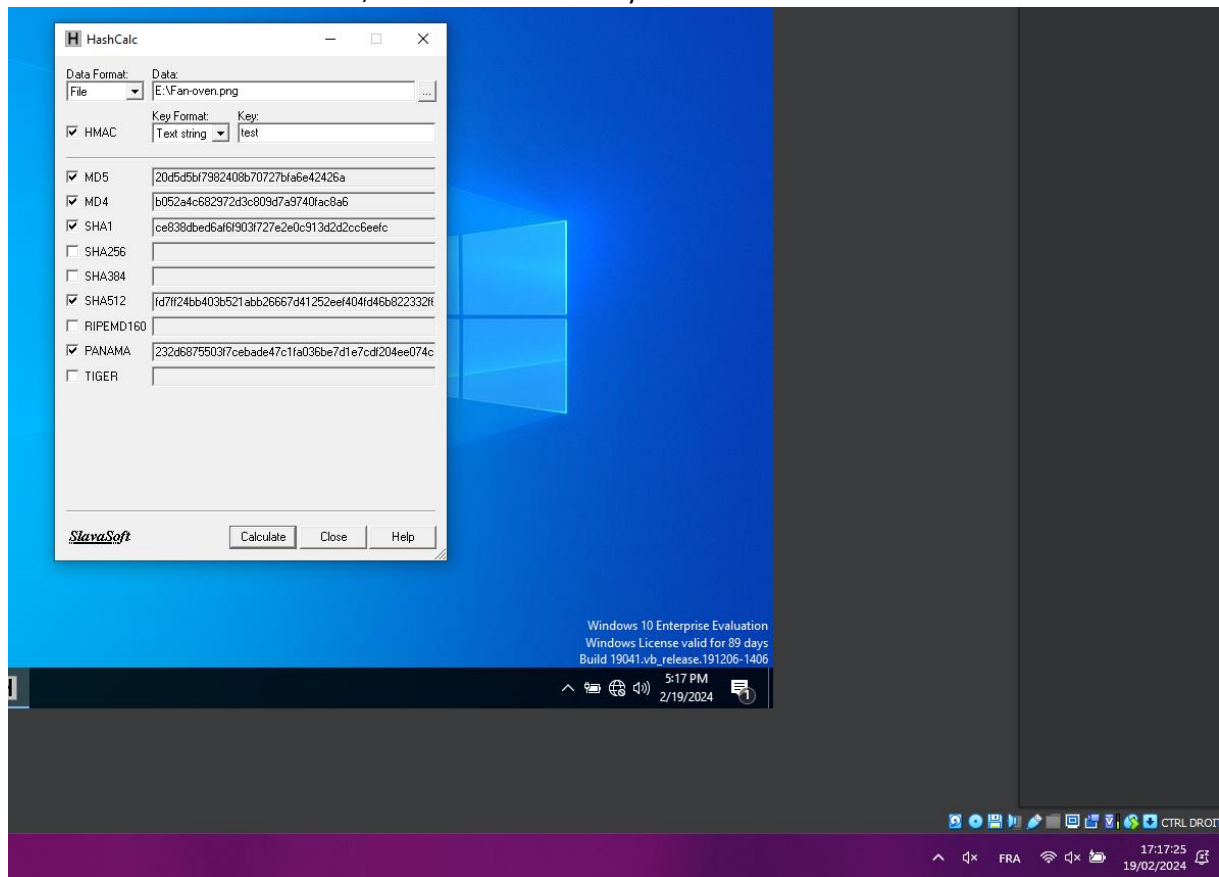
Task 2: Pre-Analysis – Determine Hash Values

With the help of the application HashCalc, I can find the hashes of files.

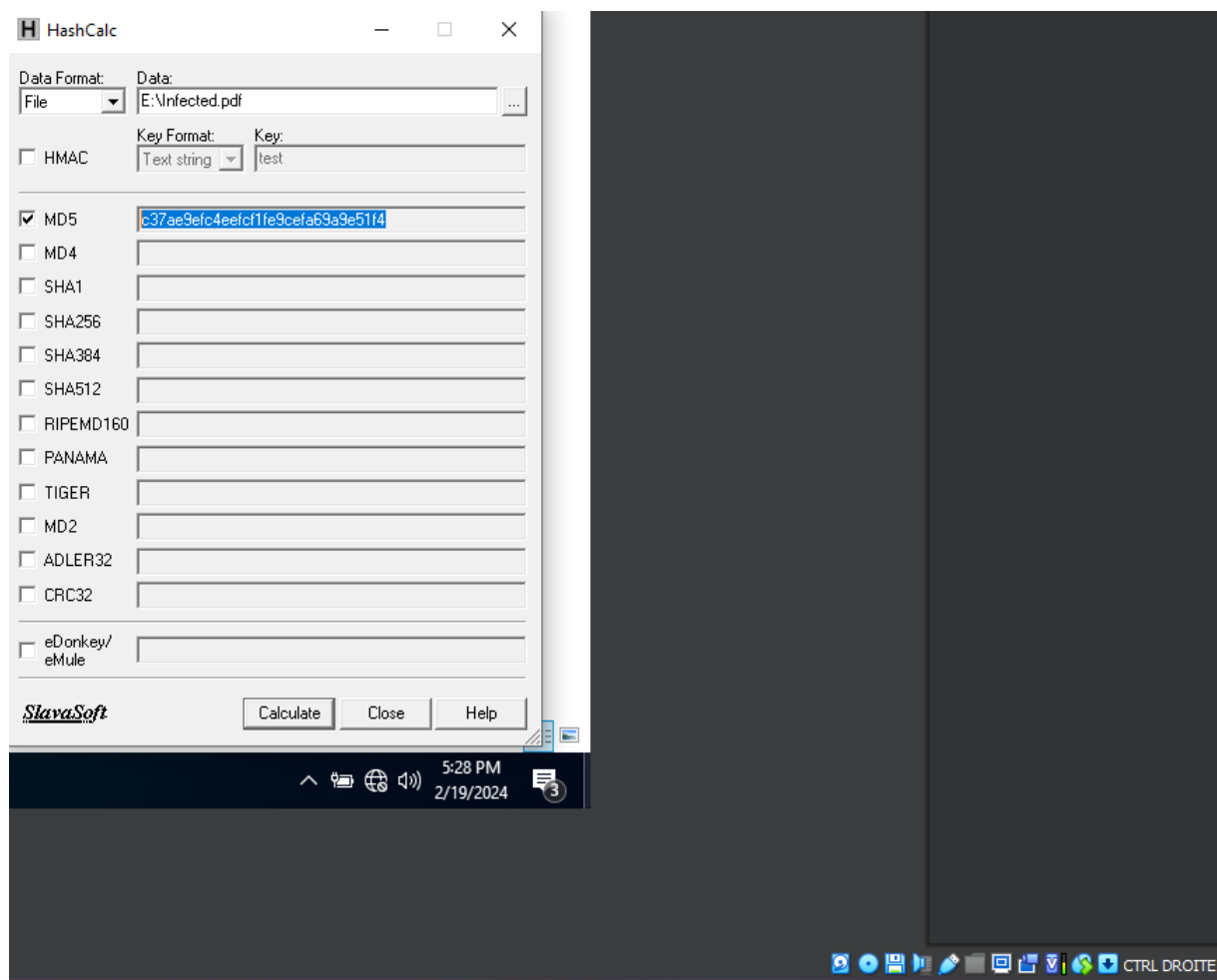
I tested the app with an image => Fan-oven.png.



If I select the HMAC checkbox, I can calculate the Keyed.



I can now do the same operation with an infected file => infected..pdf



I can now verify the danger of the file using VirusTotal and the hash I get from the file.

41
/ 61

Community Score

41 security vendors and no sandboxes flagged this file as malicious

367547f151358c3ff872bda0017ed0871842b946c7b61da5e4d91f48176a617d

Business Strategy.pdf

Size
6.61 KB

Last Analysis Date
4 days ago

PDF

pdf cve-2008-2992 runtime-modules js-embedded checks-network-adapters exploit long-sleeps autoaction checks-user-input detect-debug-environment direct-cpu-clock-access

Reanalyze Similar More

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 7

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.name/pdfka

Threat categories trojan

Family labels name pdfka expl

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Exploit/PDF.Generic.S1213	ALYac	Exploit.PDF-Name.2.Gen
Arcabit	Exploit.PDF-Name.2.Gen	Avast	JS:Pdfka-AK [Expl]
AVG	JS:Pdfka-AK [Expl]	Avira (no cloud)	HTML/Malicious.PDF.Gen3
Baidu	JS.Exploit.Pdfka.adb	BitDefender	Exploit.PDF-Name.2.Gen
ClamAV	Pdf.Dropper.Agent-6335515-0	Cynet	Malicious (score: 99)
DrWeb	PDF.CVE-2008-2992.1	Emsisoft	Exploit.PDF-Name.2.Gen (B)
eScan	Exploit.PDF-Name.2.Gen	ESET-NOD32	JS/Exploit.Pdfka.NOO
Fortinet	PDF/Script.JSSlexploit	GData	Exploit.PDF-Name.2.Gen
Google	Detected	Ikarus	Trojan.JS.Pdfka
Kaspersky	Exploit.JS.Pdfka.cil	Lionic	Trojan.PDF.Name.3/c

17:26:56
19/02/2024