

UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI
Information and Communication Technology Department



Lab Work Day 2

Digital Forensic

Name - ID: Đào Ngọc Tùng BA12-185

Trần Đức Trung BA12-179

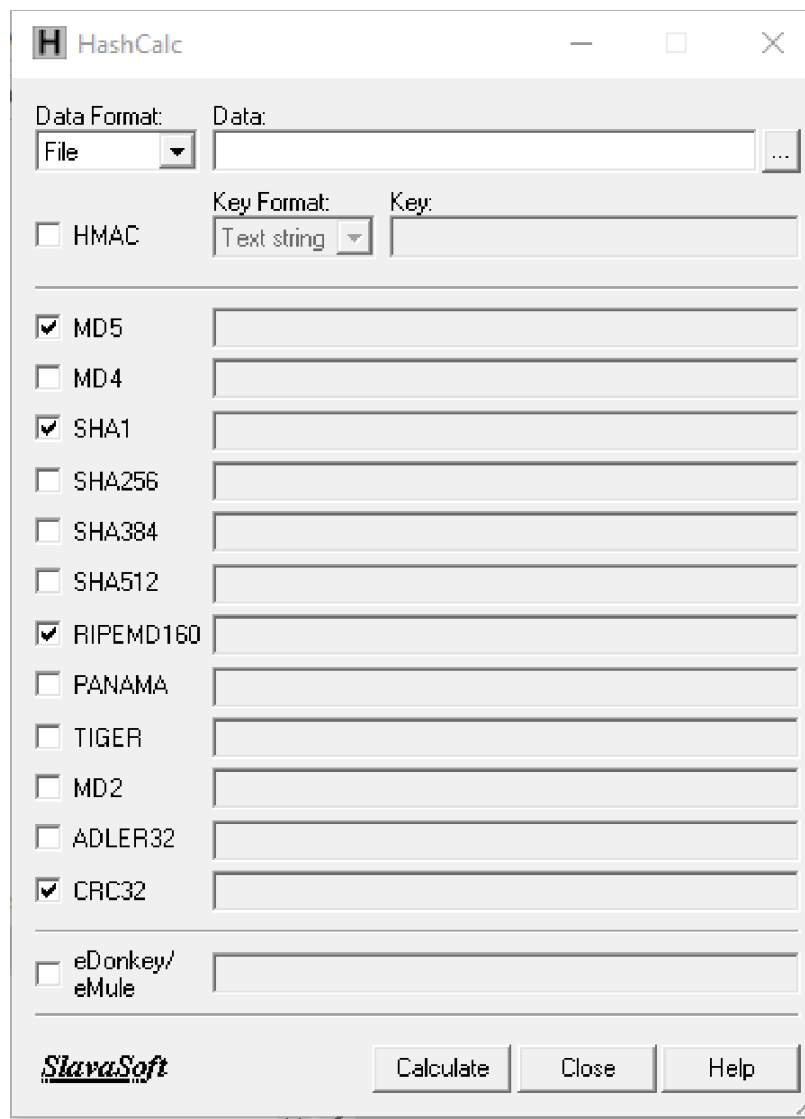
Phạm Phú Hưng BA12-081

Nguyễn Tiến Ngọc BA12-140

Ha Noi, 06 November 2024

Lab 2:

A. Launch HashCalc



B. Open Fan-oven.png and Calculate

H HashCalc

Data Format: Data: ...

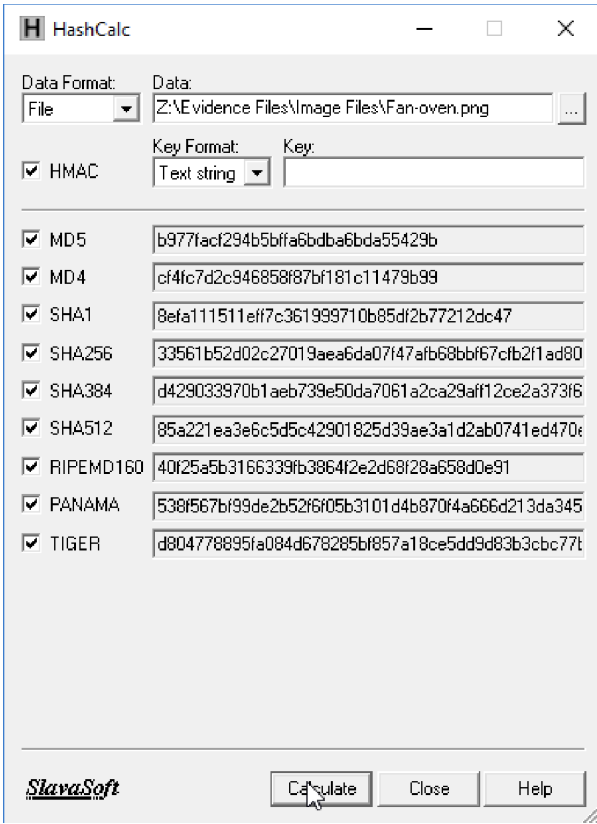
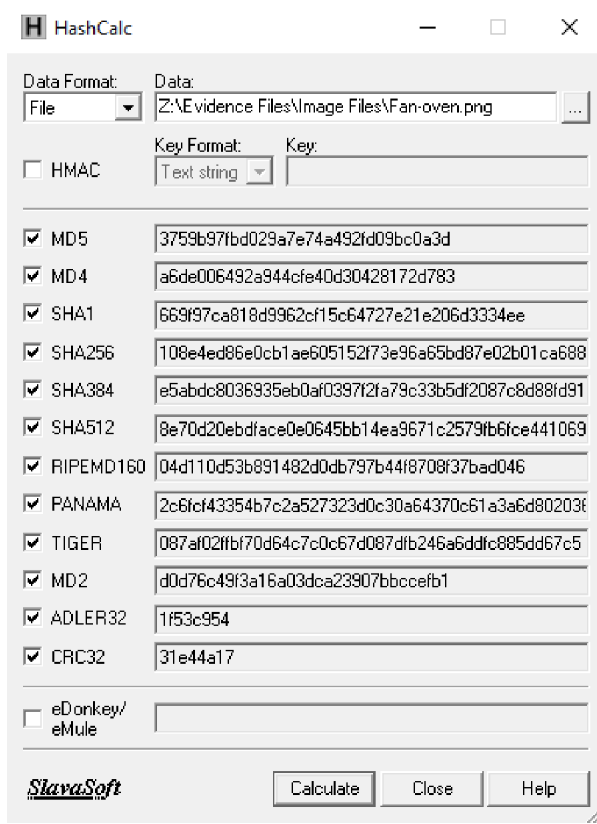
☐ HMAC Key Format: Key:

<input checked="" type="checkbox"/> MD5	<input type="text" value="3759b97fbd029a7e74a492fd09bc0a3d"/>
<input checked="" type="checkbox"/> MD4	<input type="text" value="a6de006492a944cfe40d30428172d783"/>
<input checked="" type="checkbox"/> SHA1	<input type="text" value="669f97ca818d9962cf15c64727e21e206d3334ee"/>
<input checked="" type="checkbox"/> SHA256	<input type="text" value="108e4ed86e0cb1ae605152f73e96a65bd87e02b01ca688"/>
<input checked="" type="checkbox"/> SHA384	<input type="text" value="e5abdc8036935eb0af0397f2fa79c33b5df2087c8d88fd91"/>
<input checked="" type="checkbox"/> SHA512	<input type="text" value="8e70d20ebdface0e0645bb14ea9671c2579fb6fce441069"/>
<input checked="" type="checkbox"/> RIPEMD160	<input type="text" value="04d110d53b891482d0db797b44f8708f37bad046"/>
<input checked="" type="checkbox"/> PANAMA	<input type="text" value="2c6fcf43354b7c2a527323d0c30a64370c61a3a6d802036"/>
<input checked="" type="checkbox"/> TIGER	<input type="text" value="087af02ffb70d64c7c0c67d087dfb246a6ddfc885dd67c5"/>
<input checked="" type="checkbox"/> MD2	<input type="text" value="d0d76c49f3a16a03dca23907bbccefb1"/>
<input checked="" type="checkbox"/> ADLER32	<input type="text" value="1f53c954"/>
<input checked="" type="checkbox"/> CRC32	<input type="text" value="31e44a17"/>

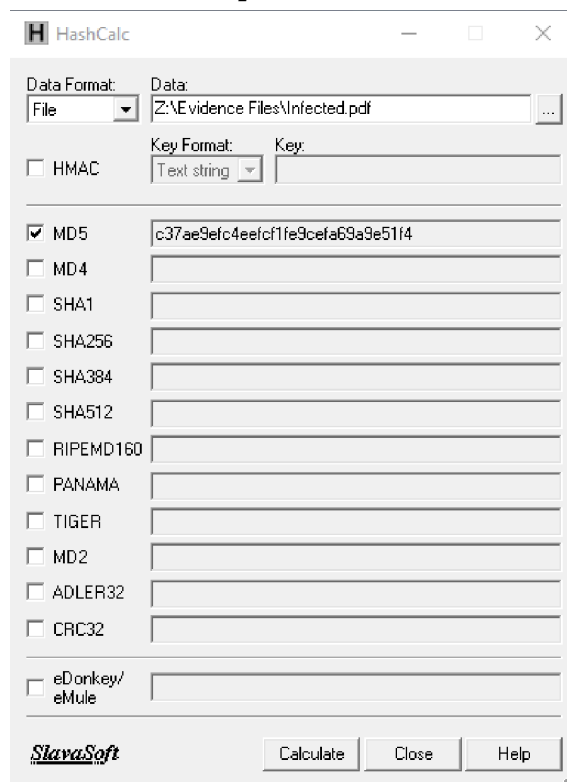
☐ eDonkey/
eMule

SlavaSoft

C. Calculate With Hmac And Not Hmac

Hmac	Not Hmac																																														
 <p>HashCalc window showing HMAC calculation results. The Data Format is set to File, and the Data is Z:\Evidence Files\Image Files\Fan-oven.png. The Key Format is set to Text string, and the Key is empty. The HMAC checkbox is checked. The results are displayed for MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, PANAMA, and TIGER algorithms.</p> <table border="1"><thead><tr><th>Algorithm</th><th>Hash</th></tr></thead><tbody><tr><td>MD5</td><td>b977facf294b5bffa6bdba6bda55429b</td></tr><tr><td>MD4</td><td>cf4fc7d2c946858f87bf181c11479b99</td></tr><tr><td>SHA1</td><td>8efa111511ef7c361999710b85df2b77212dc47</td></tr><tr><td>SHA256</td><td>33561b52d02c27019aea6da07f47afb68bbf67cfb2f1ad80</td></tr><tr><td>SHA384</td><td>d429033970b1aeb739e50da7061a2ca29aff12ce2a373f6</td></tr><tr><td>SHA512</td><td>85a221ea3e6c5d5c42901825d39ae3a1d2ab0741ed470e</td></tr><tr><td>RIPEMD160</td><td>40f25a5b3166339fb3864f2e2d68f28a658d0e91</td></tr><tr><td>PANAMA</td><td>538f567bf99de2b52f6f05b3101d4b870f4a666d213da345</td></tr><tr><td>TIGER</td><td>d804778895fa084d678285bf857a18ce5dd9d83b3cbc77t</td></tr></tbody></table>	Algorithm	Hash	MD5	b977facf294b5bffa6bdba6bda55429b	MD4	cf4fc7d2c946858f87bf181c11479b99	SHA1	8efa111511ef7c361999710b85df2b77212dc47	SHA256	33561b52d02c27019aea6da07f47afb68bbf67cfb2f1ad80	SHA384	d429033970b1aeb739e50da7061a2ca29aff12ce2a373f6	SHA512	85a221ea3e6c5d5c42901825d39ae3a1d2ab0741ed470e	RIPEMD160	40f25a5b3166339fb3864f2e2d68f28a658d0e91	PANAMA	538f567bf99de2b52f6f05b3101d4b870f4a666d213da345	TIGER	d804778895fa084d678285bf857a18ce5dd9d83b3cbc77t	 <p>HashCalc window showing calculation results. The Data Format is set to File, and the Data is Z:\Evidence Files\Image Files\Fan-oven.png. The Key Format is set to Text string, and the Key is empty. The HMAC checkbox is unchecked. The results are displayed for MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, PANAMA, TIGER, MD2, ADLER32, and CRC32 algorithms.</p> <table border="1"><thead><tr><th>Algorithm</th><th>Hash</th></tr></thead><tbody><tr><td>MD5</td><td>3759b97fbd029a7e74a492fd09bc0a3d</td></tr><tr><td>MD4</td><td>a6de006492a944cfe40d30428172d783</td></tr><tr><td>SHA1</td><td>669f97ca818d9962cf15c64727e21e206d3334ee</td></tr><tr><td>SHA256</td><td>108e4ed86e0cb1ae605152f73e96a65bd87e02b01ca688</td></tr><tr><td>SHA384</td><td>e5abdc8036935eb0af0397f2fa79c33b5df2087c8d88fd91</td></tr><tr><td>SHA512</td><td>8e70d20ebdface0e0645bb14ea9671c2579fb6fce441069</td></tr><tr><td>RIPEMD160</td><td>04d110d53b891482d0db797b44f8708f37bad046</td></tr><tr><td>PANAMA</td><td>2c6fcf43354b7c2a527323d0c30a64370c61a3a6d802036</td></tr><tr><td>TIGER</td><td>087af02ffb70d64c7c0c67d087d1b246a6ddfc885dd67c5</td></tr><tr><td>MD2</td><td>d0d76c49f3a16a03dca23907bbcccfb1</td></tr><tr><td>ADLER32</td><td>1f53c954</td></tr><tr><td>CRC32</td><td>31e44a17</td></tr></tbody></table>	Algorithm	Hash	MD5	3759b97fbd029a7e74a492fd09bc0a3d	MD4	a6de006492a944cfe40d30428172d783	SHA1	669f97ca818d9962cf15c64727e21e206d3334ee	SHA256	108e4ed86e0cb1ae605152f73e96a65bd87e02b01ca688	SHA384	e5abdc8036935eb0af0397f2fa79c33b5df2087c8d88fd91	SHA512	8e70d20ebdface0e0645bb14ea9671c2579fb6fce441069	RIPEMD160	04d110d53b891482d0db797b44f8708f37bad046	PANAMA	2c6fcf43354b7c2a527323d0c30a64370c61a3a6d802036	TIGER	087af02ffb70d64c7c0c67d087d1b246a6ddfc885dd67c5	MD2	d0d76c49f3a16a03dca23907bbcccfb1	ADLER32	1f53c954	CRC32	31e44a17
Algorithm	Hash																																														
MD5	b977facf294b5bffa6bdba6bda55429b																																														
MD4	cf4fc7d2c946858f87bf181c11479b99																																														
SHA1	8efa111511ef7c361999710b85df2b77212dc47																																														
SHA256	33561b52d02c27019aea6da07f47afb68bbf67cfb2f1ad80																																														
SHA384	d429033970b1aeb739e50da7061a2ca29aff12ce2a373f6																																														
SHA512	85a221ea3e6c5d5c42901825d39ae3a1d2ab0741ed470e																																														
RIPEMD160	40f25a5b3166339fb3864f2e2d68f28a658d0e91																																														
PANAMA	538f567bf99de2b52f6f05b3101d4b870f4a666d213da345																																														
TIGER	d804778895fa084d678285bf857a18ce5dd9d83b3cbc77t																																														
Algorithm	Hash																																														
MD5	3759b97fbd029a7e74a492fd09bc0a3d																																														
MD4	a6de006492a944cfe40d30428172d783																																														
SHA1	669f97ca818d9962cf15c64727e21e206d3334ee																																														
SHA256	108e4ed86e0cb1ae605152f73e96a65bd87e02b01ca688																																														
SHA384	e5abdc8036935eb0af0397f2fa79c33b5df2087c8d88fd91																																														
SHA512	8e70d20ebdface0e0645bb14ea9671c2579fb6fce441069																																														
RIPEMD160	04d110d53b891482d0db797b44f8708f37bad046																																														
PANAMA	2c6fcf43354b7c2a527323d0c30a64370c61a3a6d802036																																														
TIGER	087af02ffb70d64c7c0c67d087d1b246a6ddfc885dd67c5																																														
MD2	d0d76c49f3a16a03dca23907bbcccfb1																																														
ADLER32	1f53c954																																														
CRC32	31e44a17																																														

D. Open file *Infected.pdf*



E. Check *Virrruss Total*

367547f151358c3ff872bda0017ed0871842b946c7b61da5e4d91f48176a617d

47/65 security vendors flagged this file as malicious

Reanalyze Similar More

infected.pdf

Size: 6.61 KB Last Analysis Date: 8 days ago

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 15

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.pdfka/name Threat categories: trojan Family labels: pdfka name expl

Security vendors' analysis

AhnLab-V3	Exploit:PDF.Generic.S1213	AliCloud	Exploit:Javascript/Pdfka.NPX
ALYac	Exploit:PDF-Name.2.Gen	Antiy-AVL	Trojan[Exploit]/JS.Pdfka
Arcabit	Exploit:PDF-Name.2.Gen	Avast	JS:Pdfka-AK [Expl]
AVG	JS:Pdfka-AK [Expl]	Avira (no cloud)	HTML/Malicious.PDF.Gen3

Do you want to automate checks?

