

Informe de análisis forense - Anexos

Código: P04

Nombre: Bomb Threat

Equipo pericial: Grupo 3

Fecha: 04/03/2025

Índice

1. Declaración de abstención y tacha	2
2. Juramento de promesa	2
3. Figuras	3

A handwritten signature in black ink, appearing to be 'Rafael' or similar, written vertically.A handwritten signature in black ink, appearing to be 'Rafael' or similar, written horizontally.

1. Declaración de abstención y tacha

Nosotros, Grupo 3, con identificación 011002-A, en calidad de Equipo Pericial Forense Informático, declaramos formalmente lo siguiente:

1. Abstención:

No tenemos interés directo ni indirecto en los hechos objeto del presente informe pericial, ni relación alguna con las partes involucradas que pueda comprometer nuestra imparcialidad, conforme a lo establecido en la normativa ISO-27000.

2. Tacha:

Declaramos que no existen motivos de tacha que afecten nuestra idoneidad, independencia o credibilidad como peritos en este caso. No poseemos vínculos familiares, laborales ni de cualquier otra índole con las partes intervinientes.

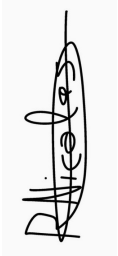

3. Confirmación de Imparcialidad:

Nuestros análisis, conclusiones y opiniones periciales se fundamentan exclusivamente en las evidencias digitales recibidas y en las metodologías técnicas reconocidas por la disciplina de informática forense, sin influencia externa de ningún tipo.

En virtud de lo anterior, asumimos la responsabilidad de actuar con total objetividad y profesionalismo en la elaboración y presentación del presente informe.

2. Juramento de promesa

Nosotros, Grupo 3, identificados con 011002-A, en calidad de Equipo de Peritaje Forense Informático, bajo juramento, prometemos solemnemente lo siguiente:

- 
1. Realizar el análisis técnico del presente caso conforme a los principios de objetividad, veracidad, y rigurosidad científica propios de la disciplina de informática forense.
 2. Garantizar que todas las conclusiones presentadas en el informe pericial se sustentan exclusivamente en las evidencias digitales analizadas y las metodologías técnicamente válidas, sin alteraciones ni omisiones deliberadas.
 3. Actuar de manera independiente e imparcial, sin recibir presiones, influencias externas o intereses personales que puedan comprometer la integridad de mi labor.
 4. Cumplir con las disposiciones legales y éticas vigentes aplicables al ejercicio de nuestra actividad como peritos, asegurando la confidencialidad de los datos y evidencias manejados durante el proceso.
- 

Declaramos bajo juramento que honraremos este compromiso en la ejecución de nuestras funciones como perito en este caso.

En Cádiz a 4 de Marzo de 2025

Fdo:



3. Figuras

- Figura 1: Verificación del hash de los archivos.

```
PS C:\Users\victo\Desktop\Bomb Threat> Get-FileHash .\DESKTOP-01S7HH9-20220408-171552.dmp -Algorithm SHA256

Algorithm Hash Path
-----
SHA256 EDCDBCAC27263A45D6DFE27F6C8BAFF55952B2357A70031DE20DE057730CD359 C:\Users\victo\Desktop\Bomb Threat\...

PS C:\Users\victo\Desktop\Bomb Threat> Get-FileHash .\DESKTOP-01S7HH9-20220408-171552.dmp.zip -Algorithm SHA256

Algorithm Hash Path
-----
SHA256 2246B2ABB178B3A508B5C8207D50E7E6F86D5C1F09487B50DAAA6387BEF639F0 C:\Users\victo\Desktop\Bomb Threat\...

PS C:\Users\victo\Desktop\Bomb Threat> Get-FileHash .\DESKTOP-01S7HH9-20220408-171552.json -Algorithm SHA256

Algorithm Hash Path
-----
SHA256 CBBD0AC591B4FC425550EB1292AD8F1DDDC4B0146A6D0DF7B23F6D13FA84B049 C:\Users\victo\Desktop\Bomb Threat\...
```

- Figura 2: Nombre del equipo

```
(nico@kali)-[~/Documentos/ ]
$ vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp --profile=Win10x64_19041 envvars | grep -i "computername"
Volatility Foundation Volatility Framework 2.6.1
524 wininit.exe 0x000001f6cf004740 COMPUTERNAME DESKTOP-01S7HH9
616 winlogon.exe 0x0000025854e76850 COMPUTERNAME DESKTOP-01S7HH9
644 services.exe 0x0000023c542027f0 COMPUTERNAME DESKTOP-01S7HH9
660 lsass.exe 0x00000254382027f0 COMPUTERNAME DESKTOP-01S7HH9
^C
```

- Figura 3: PID del proceso de la aplicación para visualizar PDFs y su proceso padre.

```
(nico@kali)-[~/Documentos/ ]
$ vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp --profile=Win10x64_19041 pstree | grep "AcroCEF"
Volatility Foundation Volatility Framework 2.6.1
0xfffff70f581eb080:AcroCEF.exe 7376 8664 0 ----- 2022-04-08 17:08:48 UTC+0000
```

- Figura 4: Documentos, más relevantes, que estaban siendo editados durante la intervención.

```
(nico@kali)-[~/Documentos/ ]
$ vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp --profile=Win10x64_19041 handles -t file | grep -E -i "(\\.docx|\\.pdf|\\.txt|\\.xlsx|\\.pptx|\\.odt|\\.ods|\\.odp)"
Volatility Foundation Volatility Framework 2.6.1
0xfffff70f5778d530 5332 0x228 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\bootstrap_log.txt
0xfffff70f58531300 5332 0x908 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\configstore_log.txt
0xfffff70f58533ba0 5332 0x924 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\systemmanager.txt
0xfffff70f5778cd60 5332 0x978 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\connection_log.txt
0xfffff70f582d77f0 5332 0xa78 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\shader_log.txt
0xfffff70f5864d780 5332 0xb14 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\steamui_system.txt
0xfffff70f58650ca0 5332 0xb48 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\controller.txt
0xfffff70f58651470 5332 0xb74 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\cloud_log.txt
0xfffff70f586504d0 5332 0xbbc 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\workshop_log.txt
0xfffff70f58651790 5332 0xbcc 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\content_log.txt
0xfffff70f5865a8e0 5332 0xc1c 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\remote_connections.txt
0xfffff70f5865a2a0 5332 0xc74 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\parental_log.txt
0xfffff70f5865eda0 5332 0xc94 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\compat_log.txt
0xfffff70f58653ea0 5332 0xcd4 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\appinfo_log.txt
0xfffff70f57fe1790 5332 0xf8c 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\stats_log.txt
0xfffff70f58512540 6300 0x31c 0x120196 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\webhelper.txt
0xfffff70f582d2cf0 6300 0x390 0x100084 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\cef_log.txt
0xfffff70f5864a580 7740 0x320 0x100084 File \\Device\\HarddiskVolume2\\Program Files (x86)\\Steam\\logs\\cef_log.txt
0xfffff70f57caa4d0 8852 0xc08 0x12019f File \\Device\\HarddiskVolume2\\Users\\Pacopepe\\Desktop\\Trabajo historia Pacopepe.odt
```

- Figura 5: Comprobación del proceso padre.

```
0xffff70f5812340 0300 0x1c 0x120190 File \Device\HarddiskVolume2\Program Files (x86)\Steam\logs\webnoper...
0xffff70f582d2cf0 6300 0x390 0x100084 File \Device\HarddiskVolume2\Program Files (x86)\Steam\logs\cef_log.txt
0xffff70f5864a580 7760 0x320 0x100084 File \Device\HarddiskVolume2\Program Files (x86)\Steam\logs\cef_log.txt
0xffff70f57caa4d0 8852 0xc08 0x12019f File \Device\HarddiskVolume2\Users\Pacopepe\Desktop\Trabajo historia Pacopepe.odt

(nico@kali) ~/Documentos
$ vol.py -f DESKTOP-0157HH9-20220408-171552.dmp --profile=Win10x64_19041 pslist | grep 8852
Volatility Foundation Volatility Framework 2.6.1
0xffff70f58764080 soffice.bin 8852 8832 13 0 1 0 2022-04-08 17:07:46 UTC+0000
```

- Figura 6: Registro bruto de la conversación en Discord.

```
atokctfucor(freatfngcngnagngncipjggtpkxoeokjnnmtkgoqatitipagoponaxmgjgkxkicoktgnbdiitanicnmkdtetoebrcegoungubg)jknagpogkxtjctfnatnfmknagadokuejnakogotidnjanjconcpndrmaguoahnatjcongenhoitucacis
kocgdbgdphmfnnkjfndebhlpacaaameehgdglancpfpcecnibhldgdeonlhdgbicnpaafndoepphoppjknknkcndngdngbgholcljnmccafekmcfmnpagpijgdblpofjaocmncblkenfeafhoahicefigdbldfngghckkbhepfaibanfiflbnlegdblnhmiljgogkaah
mmjnglmcmcnfkegdbnahlhddjofnknghfoakokiepgkqgdbpofdenkaerigkifgcdjidlgenbengdbpifgemehplijkgkghncippegbbabgds
1543934432 "components": [], {"id": "9620252476495682", "type": 0, "content": "Aud53eUdd2j", "channel_id": "961319910364020786", "author": {"id": "961318214552391710", "username": "marcosheredia666", "avatar":
"timestamp": "2022-04-08T16:25:34.832000+00:00", "edited_timestamp": null, "flags": 0, "components": []}, {"id": "962025373326016532", "type": 0, "content": "ke le den por kulo", "channel_id": "961319910364020786",
"author": {"id": "961276502417211453", "username": "pakoapepe88", "avatar": "42e461a697b1a3c802da69f75555cdbl", "discriminator": "7454", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "men
tion_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "timestamp": "2022-04-08T16:25:22.568000+00:00", "edited_timestamp": null, "flags": 0, "components": []}, {"id": "9620233699192056", "t
ype": 0, "content": "hala, ya no hai examen de lengua", "channel_id": "961319910364020786", "author": {"id": "961276502417211453", "username": "pakoapepe88", "avatar": "42e461a697b1a3c802da69f75555cdbl", "discrimi
nator": "7454", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "timestamp": "2022-04-08T16:25:19.620000+00:00",
"edited_timestamp": null, "flags": 0, "components": []}, {"id": "962025308339445850", "type": 0, "content": "si buajajaja", "channel_id": "961319910364020786", "author": {"id": "961276502417211453", "username":
"pakoapepe88", "avatar": "42e461a697b1a3c802da69f75555cdbl", "discriminator": "7454", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone":
false, "tts": false, "timestamp": "2022-04-08T16:25:07.074000+00:00", "edited_timestamp": null, "flags": 0, "components": []}, {"id": "962025265188402592", "type": 0, "content": "fuiste tu el que llanUB0f5 al in
sti con la amenaza de bombas, so colgao?", "channel_id": "961319910364020786", "author": {"id": "961318214552391710", "username": "marcosheredia666", "avatar": "7b5269335ab74dd677a14c3dbdb61c84", "discriminator":
"1465", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "timestamp": "2022-04-08T16:24:56.786000+00:00", "edited
timestamp": null, "flags": 0, "components": []}, {"id": "962023392775643146", "type": 0, "content": "bueno, yo eso si", "channel_id": "961319910364020786", "author": {"id": "961318214552391710", "username": "mar
cosheredia666", "avatar": "7b5269335ab74dd677a14c3dbdb61c84", "discriminator": "1465", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone":
false, "tts": false, "timestamp": "2022-04-08T16:17:30.368000+00:00", "edited_timestamp": null, "flags": 0, "components": []}, {"id": "962023343341580298", "type": 0, "content": "es ke ni copiar de la wikipedia
, te lo juro.", "channel_id": "961319910364020786", "author": {"id": "961276502417211453", "username": "pakoapepe88", "avatar": "42e461a697b1a3c802da69f75555cdbl", "discriminator": "7454", "public_flags": 0, "att
achments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "timestamp": "2022-04-08T16:17:18.582000+00:00", "edited_timestamp": null, "flags": 0, "c
omponents": []}, {"id": "96202324801679400", "type": 0, "content": "bah tampoco yo", "channel_id": "961319910364020786", "author": {"id": "961318214552391710", "username": "marcosheredia666", "avatar": "7b52693
35ab74dd677a14c3dbdb61c84", "discriminator": "1465", "public_flags": 0, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "timestamp":
"2022-04-08T16:17:04.625000+00:00", "edited_timestamp": null, "flags": 0, "co
1608530096 India - Bombay
1608530096 India - Bombay
```