Threat Hunting

HW07

Name: 劉定睿 ID: M11409313

Date: 2025-11-03

目錄

EXIF

- Download the raw mov video. And try to use exiftool to analysis.

```
└─$ exiftool '843cb1504c832f0d0fa6a0203047ff6d.mov'
ExifTool Version Number         : 13.25
File Name                       : 843cb1504c832f0d0fa6a0203047ff6d.mov
Directory                       : .
File Size                       : 13 MB
File Modification Date/Time     : 2025:06:21 15:58:02+08:00
File Access Date/Time           : 2025:10:29 10:59:25+08:00
File Inode Change Date/Time     : 2025:10:25 11:03:21+08:00
File Permissions                : -rwxrwxrwx
File Type                       : MOV
File Type Extension             : mov
MIME Type                       : video/quicktime
Major Brand                     : Apple QuickTime (.MOV/QT)
Minor Version                   : 0.0.0
Compatible Brands               : qt
Movie Header Version            : 0
Create Date                     : 2025:06:20 19:01:52
Modify Date                     : 2025:06:20 19:01:54
Time Scale                      : 600
Duration                        : 7.27 s
Preferred Rate                  : 1
Preferred Volume                : 100.00%
Preview Time                    : 0 s
Preview Duration                : 0 s
Poster Time                     : 0 s
Selection Time                  : 0 s
Selection Duration              : 0 s
Current Time                    : 0 s
Next Track ID                   : 3
Track Header Version            : 0
Track Create Date               : 2025:06:20 19:01:52
Track Modify Date               : 2025:06:20 19:01:54
Track ID                        : 1
```

```
Track Duration                  : 7.24 s
Track Layer                     : 0
Track Volume                    : 100.00%
Balance                         : 0
Audio Format                    : mp4a
Audio Channels                  : 2
Audio Bits Per Sample           : 16
Audio Sample Rate               : 44100
Purchase File Format            : mp4a
Matrix Structure                : 1 0 0 0 1 0 0 0 1
Image Width                     : 1080
Image Height                    : 1920
Clean Aperture Dimensions       : 1080x1920
Production Aperture Dimensions  : 1080x1920
Encoded Pixels Dimensions       : 1080x1920
Media Header Version            : 0
Media Create Date               : 2025:06:20 19:01:52
Media Modify Date               : 2025:06:20 19:01:54
Media Time Scale                : 600
Media Duration                  : 7.27 s
Media Language Code             : und
Graphics Mode                   : ditherCopy
Op Color                        : 32768 32768 32768
Handler Class                   : Data Handler
Handler Vendor ID               : Apple
Handler Description             : Core Media Data Handler
Compressor ID                   : avc1
Source Image Width              : 1080
Source Image Height             : 1920
X Resolution                    : 72
Y Resolution                    : 72
Compressor Name                 : H.264
```

```
Bit Depth                       : 24
Video Frame Rate                : 30
Lens Model (zho-US)             : iPhone SE (3rd generation) back camera 3.99mm f/1.8
Focal Length In 35mm Format (zho-US): 29
Handler Type                    : Metadata Tags
Location Accuracy Horizontal    : 35.000000
GPS Coordinates                 : 25 deg 3' 10.80" N, 121 deg 31' 23.52" E, 21.245 m Above Sea Level
Make                            : Apple
Model                           : iPhone SE (3rd generation)
Software                        : 17.6.1
Creation Date                   : 2025:01:19 13:52:52+08:00
Media Data Size                 : 12721092
Media Data Offset               : 6706
Lens Model                      : iPhone SE (3rd generation) back camera 3.99mm f/1.8
Focal Length In 35mm Format     : 29
Image Size                      : 1080x1920
Megapixels                      : 2.1
Avg Bitrate                     : 14 Mbps
GPS Altitude                    : 21.245 m
GPS Altitude Ref                : Above Sea Level
GPS Latitude                    : 25 deg 3' 10.80" N
GPS Longitude                   : 121 deg 31' 23.52" E
Rotation                        : 0
GPS Position                    : 25 deg 3' 10.80" N, 121 deg 31' 23.52" E
Lens ID                         : iPhone SE (3rd generation) back camera 3.99mm f/1.8
```

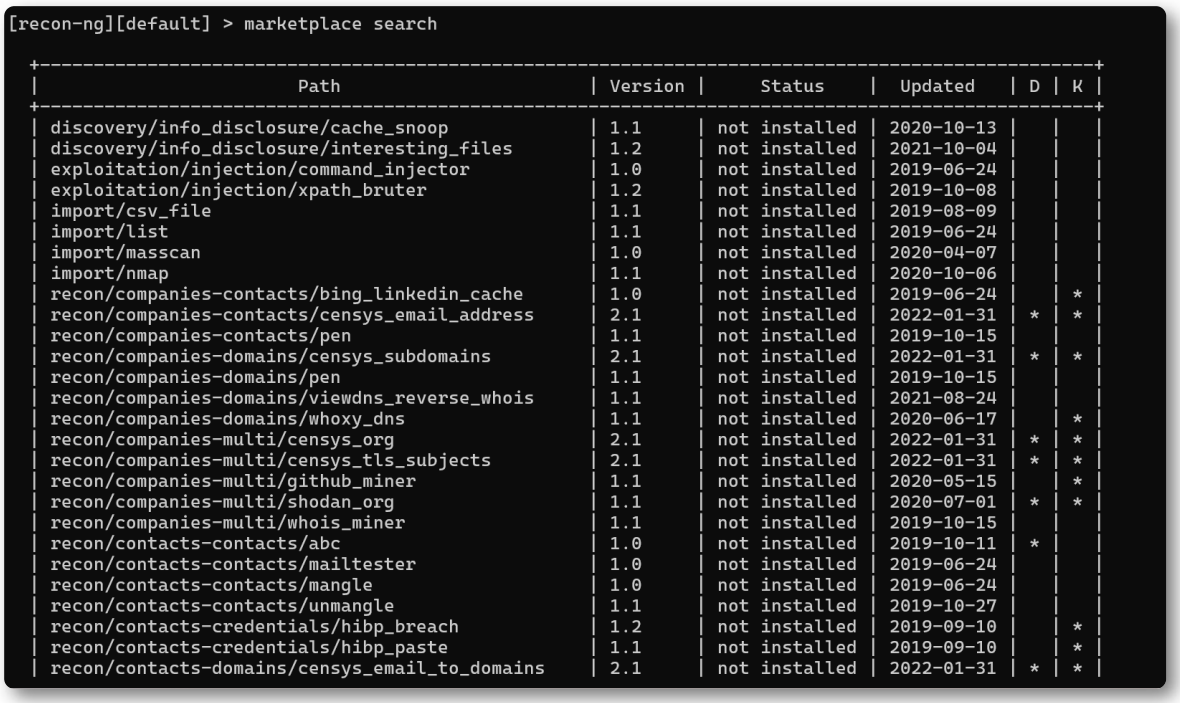
- We can see the geolocation that this video shot.

- So vibe coding a static website and used Openstreetmap API to locate the place.

recon-ng

- Initalize the recon-ng.

- use `marketplace` to search the module which I can use.



- Download the module.

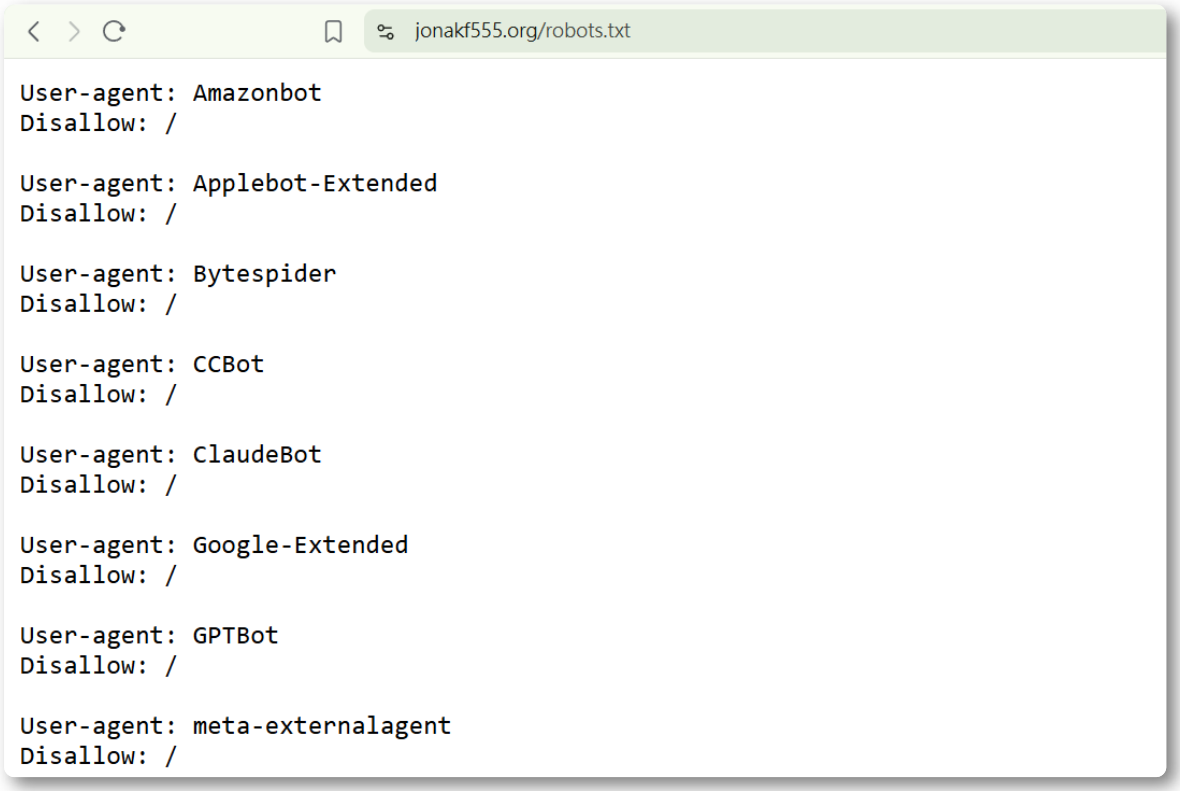
```
[recon-ng][default] > marketplace help
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules...
[recon-ng][default] >
```

- set the module's options.

- And run the module. Find the leak information on `jonakf555.org` website.

```
[recon-ng][default][interesting_files] > options set SOURCE jonakf555.org
SOURCE => jonakf555.org
[recon-ng][default][interesting_files] > run
[*] http://jonakf555.org:80/robots.txt => 200. 'robots.txt' found!
[*] http://jonakf555.org:80/sitemap.xml => 200. 'sitemap.xml' found but unverified.
[*] http://jonakf555.org:80/sitemap.xml.gz => 200. 'sitemap.xml.gz' found but unverified.
[*] http://jonakf555.org:80/crossdomain.xml => 200. 'crossdomain.xml' found but unverified.
[*] http://jonakf555.org:80/phpinfo.php => 200. 'phpinfo.php' found but unverified.
[*] http://jonakf555.org:80/test.php => 200. 'test.php' found but unverified.
[*] http://jonakf555.org:80/elmah.axd => 200. 'elmah.axd' found but unverified.
[*] http://jonakf555.org:80/server-status => 200. 'server-status' found but unverified.
[*] http://jonakf555.org:80/jmx-console/ => 200. 'jmx-console/' found but unverified.
[*] http://jonakf555.org:80/admin-console/ => 200. 'admin-console/' found but unverified.
[*] http://jonakf555.org:80/web-console/ => 200. 'web-console/' found but unverified.
[*] 1 interesting files found.
[*] Files downloaded to '/home/jonafk555/.recon-ng/workspaces/default/'
```

- browse the leak info.



Kestrel

-

1. How to use `NEW` command to create entities in a Kestrel variable? ¶

```
all_software = NEW process [
    {"name": "chrome.exe", "pid": 8888, "version": "105.0"},
    {"name": "notepad.exe", "pid": 2233, "version": "10.0"},
    {"name": "WINWORD.EXE", "pid": 5544, "version": "16.0"}
]
```

Block Executed in 1 seconds

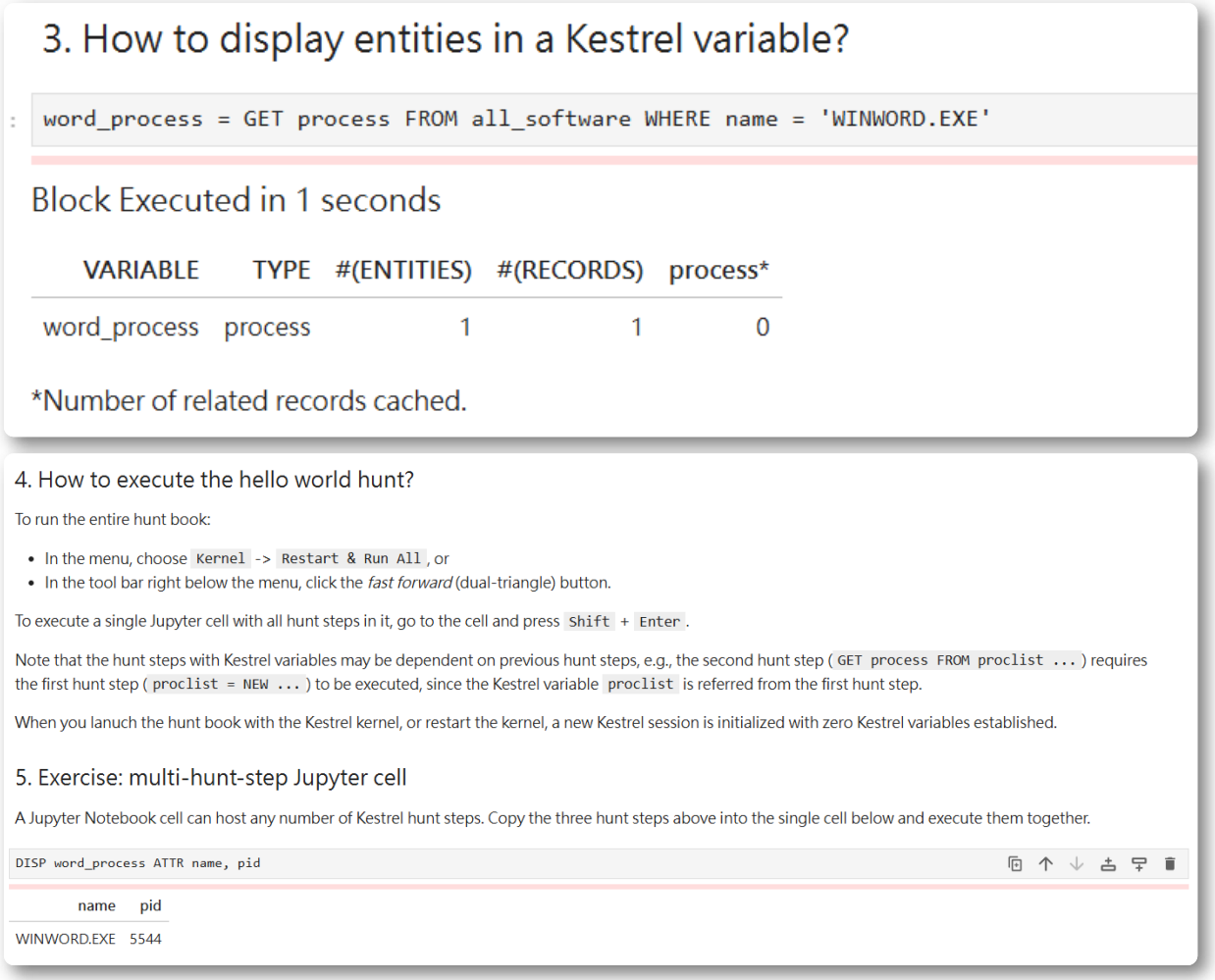
VARIABLE	TYPE	#(ENTITIES)	#(RECORDS)	process*
all_software	process	3	3	0

*Number of related records cached.

2. How to use `GET` command to retrieve a set of entities from a Kestrel variable?

```
DISP all_software ATTR name, pid, version
```

name	pid	version
notepad.exe	2233	10.0
WINWORD.EXE	5544	16.0
chrome.exe	8888	105.0



Simulate a Real-world case

```
all_logs = NEW process [
    {"name": "OUTLOOK.EXE", "pid": 3104, "id": "process--outlook"},
    {"name": "explorer.exe", "pid": 1820, "id": "process--explorer"},
    {"name": "svchost.exe", "pid": 988, "id": "process--svchost-legit"},

    # The initial malicious payload, dropped by Outlook
    {"name": "Urgent_Invoice_Q4.exe", "pid": 5560, "id": "process--invoice-malware", "parent_ref": "process--outlook"},

    # The malware spawns cmd.exe to run a discovery command
    {"name": "cmd.exe", "pid": 6012, "id": "process--cmd-child", "parent_ref": "process--invoice-malware", "command_line": "cmd.exe /c net user /domain"}

    # The malware then uses PsExec for lateral movement to a server
    {"name": "PsExec.exe", "pid": 6080, "id": "process--psexec", "parent_ref": "process--invoice-malware", "command_line": "PsExec.exe \\\\FILESRV01 -u a

    # Benign process on the remote server
    {"name": "services.exe", "pid": 744, "id": "process--filesrv-services", "hostname": "FILESRV01"},

    # The laterally moved process on the file server, created by services.exe (typical for PsExec)
    {"name": "cmd.exe", "pid": 4321, "id": "process--filesrv-cmd", "parent_ref": "process--filesrv-services", "hostname": "FILESRV01"}
]
```

Block Executed in 1 seconds

VARIABLE	TYPE	#(ENTITIES)	#(RECORDS)	process*
all_logs	process	8	8	0

*Number of related records cached.

```
# Hypothesis: An Office application spawned an unusual executable.
# 1. Find all Office processes.
office_procs = GET process FROM all_logs WHERE name = 'OUTLOOK.EXE'

# 2. Find any process created directly by those Office processes.
suspicious_children = FIND process CREATED office_procs

# 3. We now have our initial point of entry.
DISP suspicious_children ATTR name, pid, parent_ref.name
```

Block Executed in 1 seconds

VARIABLE	TYPE	#(ENTITIES)	#(RECORDS)	process*
office_procs	process	1	1	0
suspicious_children	process	0	0	0

*Number of related records cached.

```
# --- The Original, More Direct Method ---

# 1. Find the PsExec process based on the internal alert.
psexec_proc = GET process FROM all_logs WHERE name = 'PsExec.exe'

# 2. Find its parent process. This is the correct syntax.
# "RETURN parent" reverses the search to find the creator.
culprit_parent = FIND process CREATED psexec_proc

# 3. Display the source of the malicious activity.
DISP culprit_parent ATTR name, pid
```

	name	pid
	Urgent_Invoice_Q4.exe	5560

Block Executed in 1 seconds

VARIABLE	TYPE	#(ENTITIES)	#(RECORDS)	process*
psexec_proc	process	1	1	0
culprit_parent	process	1	1	0

*Number of related records cached.