

Digital Forensics

Rapport en Digital Forensics & Velociraptor

Rédiger par :
Yahya El Ourdighi
Ayoub El Mejdoub

Date :
2/8/2023

Contents

Digital Forensics.....
Avantages.....
Ex: Velociraptor
Principales caractéristiques.....
Lab de travail.....
Architecture.....
VQL Language.....
Installation.....
Nous travail (scénario).....
Conclusion.....



Digital Forensics

Digital Forensics est la procédure qui identifie et obtient des données, les traite, les analyse et les stocke pour les utiliser comme preuve dans une salle d'audience. Les preuves électroniques sont un aspect crucial de toute enquête criminelle que les professionnels peuvent collecter à partir d'appareils électroniques, tels que des ordinateurs, des smartphones, des périphériques USB, des disques durs et bien d'autres.

Comprendre divers aspects techniques du sujet est crucial si vous souhaitez poursuivre une carrière en médecine légale. Dans cet article, nous discutons de ce qu'est la criminalistique numérique et comprenons ses avantages et ses inconvénients, ainsi que des exemples.

Les Avantages de digital Forensics :

Il aide au traitement des données. Grâce à la criminalistique numérique, les enquêteurs peuvent récupérer, examiner et stocker des données et des appareils électroniques afin de leur offrir la possibilité d'utiliser les données comme preuve lors de procès devant un tribunal.

Il aide à résoudre des cas. Les agences peuvent utiliser la criminalistique numérique pour déduire l'identité de l'auteur et identifier les raisons de commettre le crime.

Il facilite la collecte précise des preuves. La criminalistique aide à créer des pratiques normalisées et des étapes à suivre lors de la collecte de preuves, ce qui garantit que la valeur et la légitimité des preuves numériques et électroniques ne sont pas compromises.

Il est utile pour récupérer et extraire des données. Les auteurs ont souvent recours à la suppression des données lorsqu'ils risquent d'être arrêtés par les autorités. Les équipes médico-légales peuvent aider à récupérer les données supprimées et extraire les fichiers cachés des appareils électroniques qui peuvent être cruciaux pour poursuivre les auteurs et aider à constituer un dossier solide contre eux dans une salle d'audience.

Cela permet d'évaluer l'ampleur du crime. Les données peuvent être un élément de preuve essentiel qui peut aider l'organisme d'enquête à déterminer l'étendue des crimes commis par les auteurs.

Il est essentiel pour créer et maintenir des rapports. Les équipes médico-légales créent et maintiennent souvent des rapports sur les enquêtes en cours et terminées et conservent des enregistrements de toutes les preuves recueillies pour faciliter l'affaire et poursuivre les auteurs.

Cela peut aider à stocker et à conserver les preuves. Le service médico-légal rassemble et stocke généralement toutes les preuves numériques sur des disques, des disques durs, des clés USB et des serveurs pour aider les agences d'enquête à résoudre l'affaire et à appréhender efficacement les suspects.

Les types de digital Forensics :



Informatique judiciaire :

Ce type de criminalistique concerne les données stockées dans les ordinateurs, les ordinateurs portables et les disques durs en récupérant, analysant et conservant les données à utiliser comme preuve. Les procédures pénales et civiles peuvent utiliser ces preuves. La criminalistique informatique et la récupération de données suivent des étapes similaires avec quelques étapes et exigences supplémentaires. Ces étapes supplémentaires garantissent que ces professionnels ont collecté les données légalement. L'informatique judiciaire fait partie intégrante de toute enquête, car elle aide les agences à récupérer des preuves cruciales qui peuvent les aider à attraper les auteurs.

Les types de digital Forensics :

Les appareils mobiles deviennent les appareils préférés des auteurs pour stocker et collecter des informations. La criminalistique mobile analyse et récupère les données stockées dans les smartphones, les tablettes, les assistants numériques personnels et les clés USB. Il existe une variété d'outils que le service médico-légal peut utiliser pour extraire des preuves à partir d'appareils mobiles, comme des logiciels de récupération de données, des acquisitions de fichiers et d'autres techniques. En raison de l'ampleur de l'utilisation des appareils mobiles, il n'existe pas qu'une seule procédure standardisée pour en extraire les données. Les experts en criminalistique suivent une série d'exercices de formation pour extraire efficacement les données des appareils mobiles et opèrent selon les directives légales pendant que l'enquête progresse.



Forensics réseaux et logiciels

La criminalistique réseau examine, collecte, récupère et stocke les données des réseaux et des serveurs en ligne. Les enquêteurs médico-légaux peuvent obtenir des données et des preuves en analysant des serveurs, des systèmes de stockage basés sur le cloud, des bases de données de messagerie et d'autres systèmes logiciels et réseaux utilisés pour stocker des informations. La criminalistique des réseaux et des logiciels se concentre sur l'observation, l'examen et le suivi du trafic du réseau informatique pour la collecte de données, d'informations et de preuves. Les réseaux peuvent également détecter si les criminels ont compromis un réseau par le biais de cyberattaques ou de virus. Les données sont constamment transmises par le biais de réseaux informatiques, ce qui fait de la criminalistique réseau une forme stimulante et dynamique de criminalistique.



Les types de Digital Forensics :

Analyse médico-légale des données

Les analystes de données médico-légales examinent, collectent et stockent des données et des preuves et les surveillent pour prévenir les crimes financiers et les activités illégales. Cette forme de criminalistique numérique se concentre sur l'analyse et la collecte de données pour rechercher des signes ou des indications d'activités frauduleuses des auteurs. Il se concentre également sur le suivi des transactions qui signalent une fraude et d'autres activités illégales. L'analyse des données médico-légales est essentielle pour les agences d'enquête lorsqu'elles enquêtent sur le blanchiment d'argent et d'autres crimes financiers.



Forensique de la base de données

L'investigation des bases de données est le type d'investigation liée aux bases de données et à leurs métadonnées. Un examen médico-légal des bases de données peut également porter sur les horodatages d'une base de données. Les services de criminalistique analysent la base de données pour vérifier si les actions de l'utilisateur de la base de données étaient dans les limites légales ou non. Cela diffère considérablement des données non structurées qui sont généralement récupérées à partir d'appareils et de logiciels de communication, d'applications de bureau et d'autres appareils mobiles. Les services d'investigation informatique ou mobile analysent, récupèrent et stockent généralement les preuves pour l'investigation des bases de données.





VELOCIRAPTOR

INTRODUCTION

Un exemple de digital forensics Framework c'est **Velociraptor IR Framework** est un framework open source de réponse aux incidents et d'investigation numérique. Il fournit une plate-forme unifiée pour les intervenants en cas d'incident, les analystes de sécurité et les enquêteurs médico-légaux pour collecter et analyser des données provenant de plusieurs sources de manière rapide, efficace et automatisée.

La puissance et la flexibilité de Velociraptor proviennent du langage de requête Velociraptor (VQL). VQL est une infrastructure de création d'artefacts hautement personnalisés, qui vous permet de collecter, d'interroger et de surveiller presque tous les aspects d'un point de terminaison, de groupes de points de terminaison ou d'un réseau entier. Il peut également être utilisé pour créer des règles de surveillance continue sur le point de terminaison, ainsi que pour automatiser les tâches sur le serveur.

Principales caractéristiques

Collecte de données automatisée : Velociraptor peut collecter des données à partir de diverses sources telles que des terminaux, des périphériques réseau, des services cloud, etc. Les données collectées peuvent inclure des données volatiles et persistantes, et elles peuvent être configurées pour inclure des types de fichiers spécifiques, des clés de registre et d'autres données.

The screenshot shows the Velociraptor interface with the following details:

Header: Search clients, PC-Statginaire.localdomain Connected, admin

Main Table: Shows a list of artifacts collected from three flows (FlowId: F.CFGBAMSBRL7K, F.CFGBAB2RSF692, F.CF55QU053G1HQ). Columns include State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows. The table has 6 rows.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CFGBAMSBRL7K	Windows.System.PowerShell	2023-02-06T08:07:55Z	2023-02-06T08:07:56Z	admin	1	1
✓	F.CFGBAB2RSF692	Windows.System.PowerShell	2023-02-06T08:07:08Z	2023-02-06T08:07:10Z	admin	1	1
✓	F.CF55QU053G1HQ	Generic.Client.Info	2023-01-28T09:23:07Z	2023-01-28T09:23:08Z	InterrogationService	1	1

Bottom Navigation: Artifact Collection (selected), Uploaded Files, Requests, Results, Log, Notebook

Left Sidebar: Overview, Artifact Names, Flow ID, Creator, Create Time, Start Time, Last Active, Duration, State, Ups/Sec, CPU Limit, IOPS Limit, Timeout.

Right Panel: Results, Available Downloads

Capacités de recherche avancées : Velociraptor fournit un puissant moteur de recherche qui vous permet de rechercher rapidement des artefacts spécifiques dans l'ensemble de votre environnement. Vous pouvez rechercher des mots-clés, des chaînes, des expressions régulières et d'autres types de données, et vous pouvez limiter vos recherches à des plages de temps spécifiques, des types de fichiers, etc.

The screenshot shows the Velociraptor interface with the following details:

Header: RH, PC-Statginaire.localdomain 1 minutes ago, admin

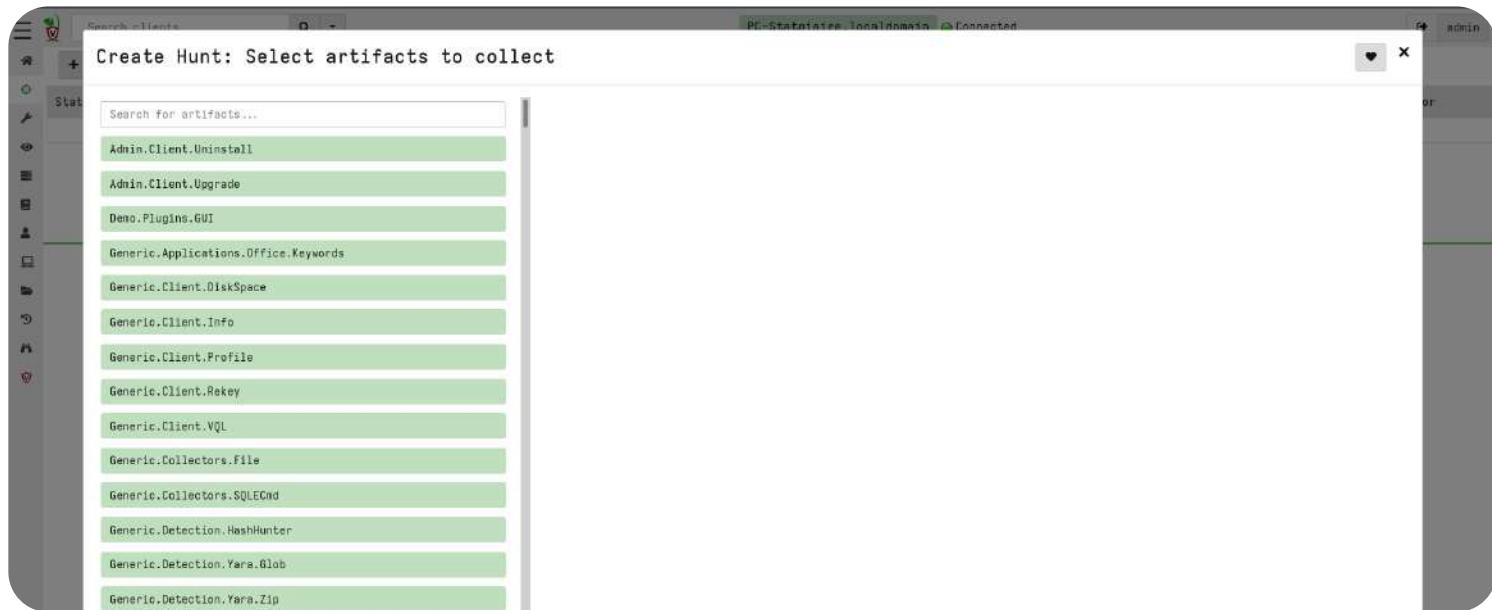
Search Bar: label:RH

Main Table: Shows a list of clients. Columns include Client ID, Hostname, FQDN, OS Version, and Labels. One client (Client ID: C.ce131ab6e13aad34) is selected. The table has 1 row.

Client ID	Hostname	FQDN	OS Version	Labels
C.ce131ab6e13aad34	PC-Statginaire	PC-Statginaire.localdomain	Microsoft Windows 10 Education 10.0.19045 Build 19045	RH

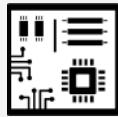
Bottom Navigation: 10, 25, 30, 50, B, Go to Page

Intégration avec d'autres outils : Velociraptor s'intègre à un large éventail d'autres outils et plates-formes, notamment des plates-formes de réponse aux incidents, des flux de renseignements sur les menaces, etc. Cela vous permet de tirer parti des atouts de plusieurs outils et plates-formes pour améliorer votre réponse aux incidents et vos capacités d'investigation.



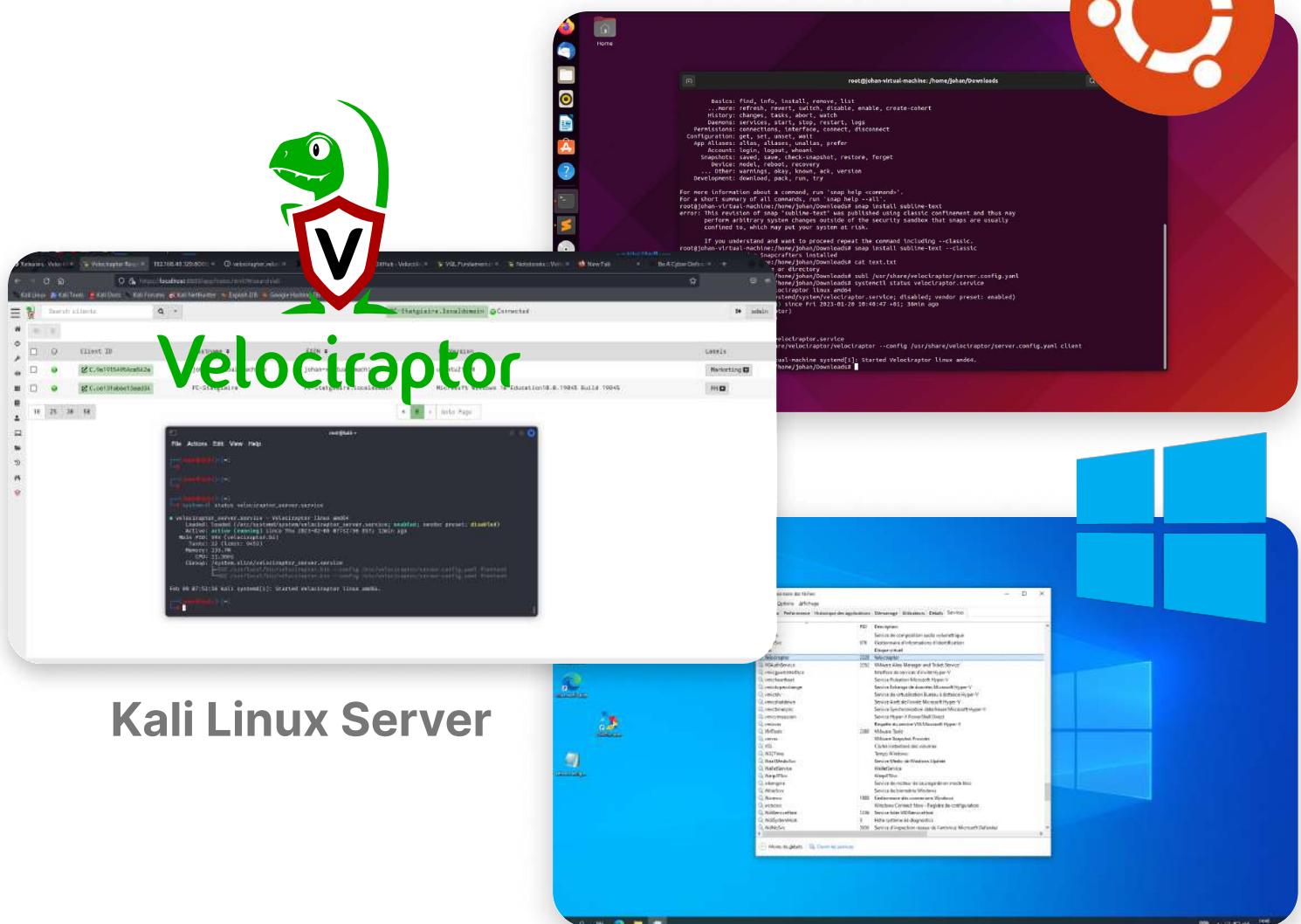
Gestion centralisée : Velociraptor fournit une console de gestion centralisée qui facilite le déploiement, la gestion et la surveillance de vos agents Velociraptor. Vous pouvez facilement afficher des informations sur l'état de vos agents, afficher les journaux et les alertes, et effectuer d'autres tâches de gestion.

Client ID	Hostname	FQDN	DS Version	Labels
C.9e19154954ce542a	johan-virtual-machine	johan-virtual-machine	ubuntu21.10	
C.ce131ab6e13aad34	PC-Statglaire	PC-Statglaire.localdomain	Microsoft Windows 10 Education 10.0.19045 Build 19045	

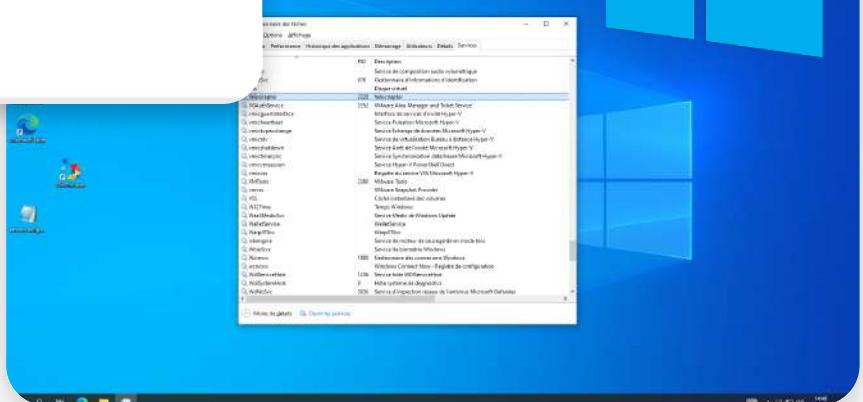


LAB DE TRAVAIL

Ubuntu 18.04 Client



Kali Linux Server



Windows 10 Client

Client:

```
server_urls:  
- https://192.168.49.129:8888/  
...
```

API:

```
bind_address 192.168.49.129
```

...

GUI:

```
bind_address: 192.168.49.129
```

...

Monitoring:

```
bind_address: 192.168.49.129
```

Architecture

L'extrémité avant

Recevoir des connexions de clients
Message de file d'attente aux clients
Traiter les réponses des clients (flux)

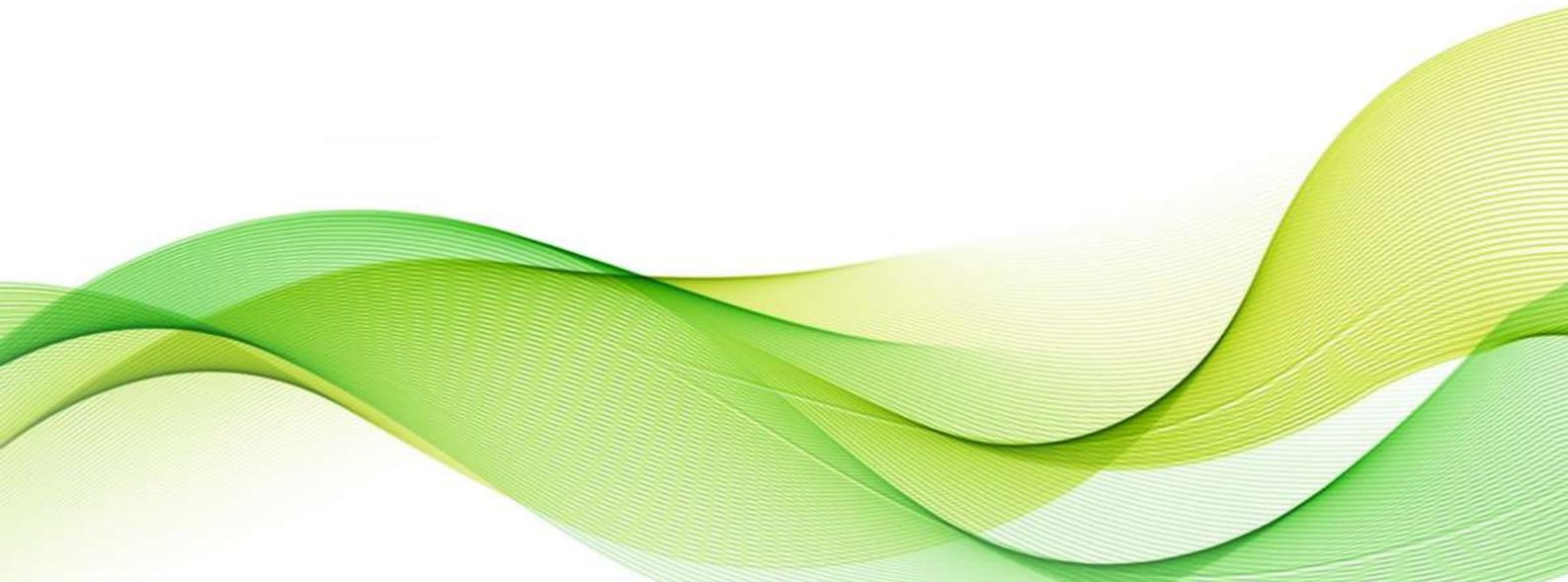
interface graphique GUI

Autoriser la planification des flux/recherches
Inspecter les résultats des flux/recherches
Afficher le système de fichiers virtuel du client

Qu'est-ce que VQL

Velociraptor Query Language (VQL) est un langage de requête expressif conçu pour adapter facilement vos besoins sans apporter de modifications aux codes, à la requête ou aux artefacts ni déployer de logiciel supplémentaire.

VQL encapsule l'expertise en criminalistique numérique dans des fichiers lisibles par l'homme appelés « artefacts » qui peuvent être partagés et échangés librement au sein de la communauté.



Installation de Velociraptor

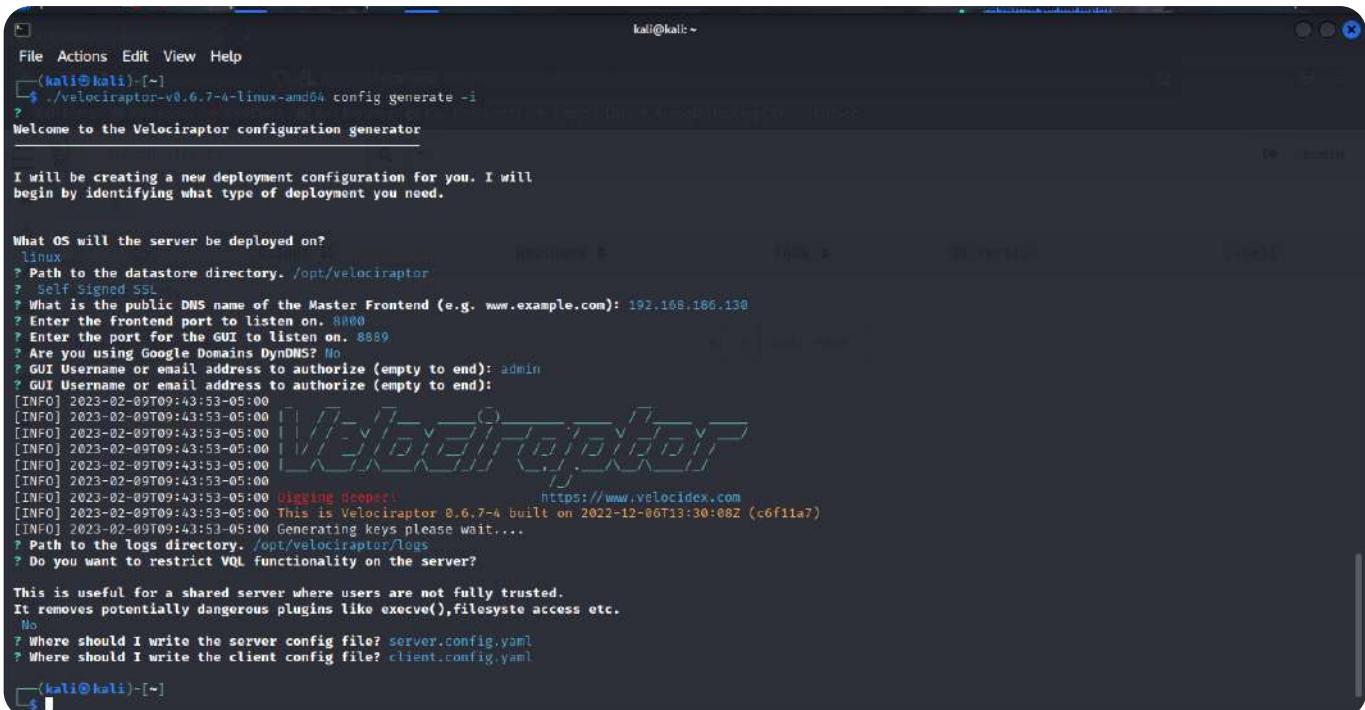
Installez Velociraptor en obtenant le binaire Linux

Assets			
 velociraptor-v0.6.7-4-darwin-amd64	52.9 MB	Dec 6, 2022	
 velociraptor-v0.6.7-4-darwin-amd64.sig	438 Bytes	Dec 6, 2022	
 velociraptor-v0.6.7-4-darwin-arm64	51.6 MB	Dec 6, 2022	
 velociraptor-v0.6.7-4-darwin-arm64.sig	438 Bytes	Dec 6, 2022	
 velociraptor-v0.6.7-4-freebsd-amd64	48.4 MB	Dec 6, 2022	
 velociraptor-v0.6.7-4-freebsd-amd64.sig	438 Bytes	Dec 6, 2022	
 velociraptor-v0.6.7-4-linux-amd64	48.2 MB	Dec 6, 2022	
 velociraptor-v0.6.7-4-linux-amd64-musl	48.3 MB	Dec 6, 2022	
 velociraptor-v0.6.7-4-linux-amd64-musl.sig	438 Bytes	Dec 6, 2022	
 velociraptor-v0.6.7-4-linux-amd64.sig	438 Bytes	Dec 6, 2022	

Rendre le binaire exécutable

```
[root@kali) ~]# chmod +x velociraptor-v0.6.7-4-linux-amd64  
[root@kali) ~]# ls  
client.config.yaml  go  server.config.yaml  velociraptor_0.6.7-4_server.deb  velociraptor-v0.6.7-4-linux-amd64  
[root@kali) ~]#
```

Générer un fichier de configuration du serveur



Générer le serveur debian à partir du fichier de configuration que nous générions

```
[root@kali]# ./velociraptor-v0.6.7-4-linux-amd64 --config server.config.yaml debian server
Creating a package for velociraptor_0.6.7-4_server.deb
[root@kali]#
```

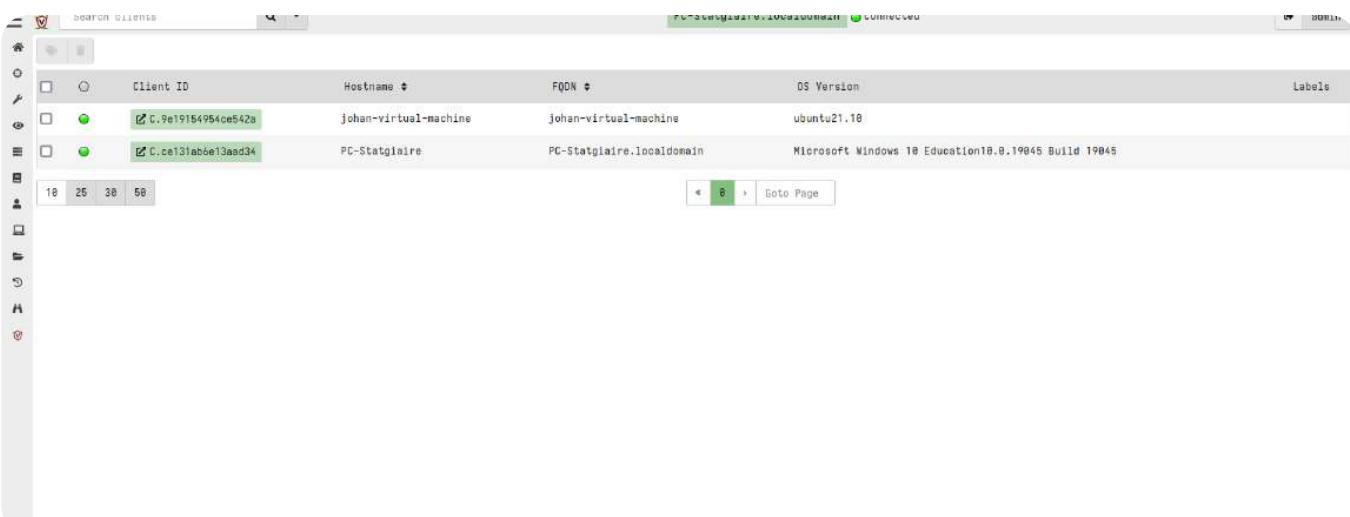
Installer le serveur debian :

```
[root@kali]# dpkg -i velociraptor_0.6.7-4_server.deb
(Reading database ... 387114 files and directories currently installed.)
Preparing to unpack velociraptor_0.6.7-4_server.deb ...
Removed "/etc/systemd/system/multi-user.target.wants/velociraptor_server.service".
```

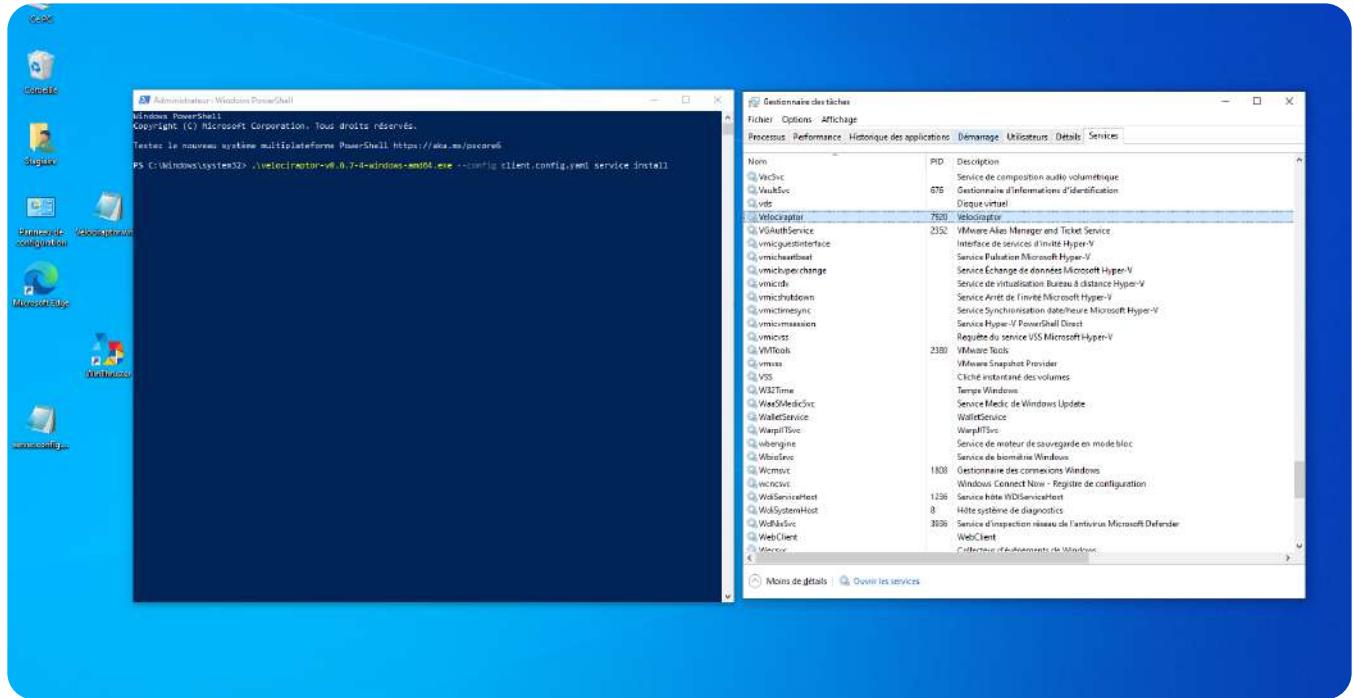
Démarrer le service de Vélociraptor systemctl

```
[root@kali]# systemctl start velociraptor_server.service
[root@kali]# systemctl status velociraptor_server.service
● velociraptor_server.service - Vélociraptor linux amd64
   Loaded: loaded (/etc/systemd/system/velociraptor_server.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2023-02-10 04:06:19 EST; 10s ago
       Main PID: 84812 (velociraptor.bi)
          Tasks: 18 (limit: 9452)
        Memory: 79.2M
         CPU: 4.971s
        CGroup: /system.slice/velociraptor_server.service
                  └─84812 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend
                     ├─84820 /usr/local/bin/velociraptor bin --config /etc/velociraptor/server.config.yaml frontend
```

Nous avons Kali comme serveur

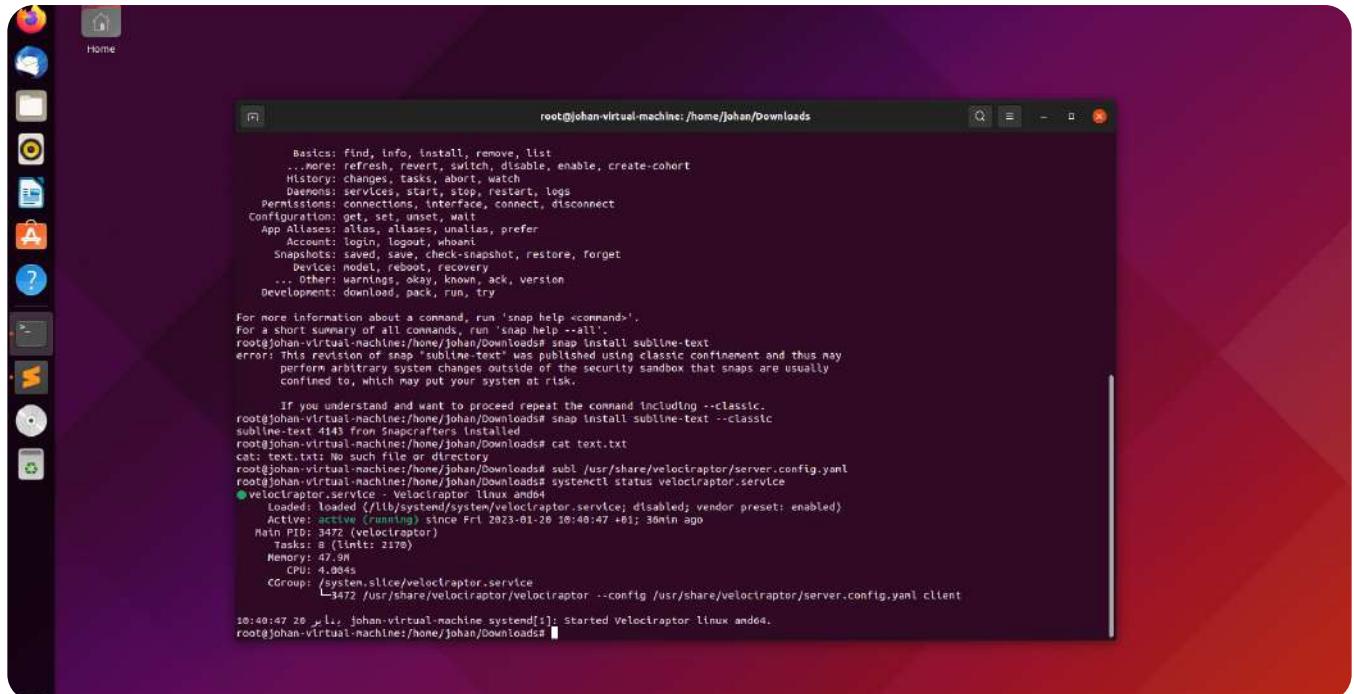


Ici nous avons windows 10 comme client 1 :



nous déployons windows en tant que client pour notre serveur kali, et nous l'ajoutons en tant que service en arrière-plan

Ici nous avons Ubuntu comme client 2 :



nous déployons ubuntu en tant que client pour notre serveur kali, et nous l'ajoutons en tant que service en arrière-plan

Artifacts

1. Artifacts du système de fichiers : Velociraptor peut collecter les métadonnées du système de fichiers, les hachages, les horodatages et même le contenu des fichiers du système cible.
2. Artifacts de mémoire : Velociraptor peut collecter des vidages de mémoire, analyser la mémoire à la recherche d'artefacts malveillants et extraire des informations de la mémoire de processus.
3. Artifacts réseau : Velociraptor peut collecter des informations de connexion réseau, y compris les connexions actives, les ports d'écoute et la configuration réseau.
4. Artifacts de processus : Velociraptor peut collecter des informations sur les processus en cours d'exécution, y compris les listes de processus, les arguments de ligne de commande et les bibliothèques chargées.
5. Artifacts de registre : Velociraptor peut collecter des informations à partir du registre Windows, y compris les entrées de démarrage automatique, les informations d'installation du logiciel et les préférences de l'utilisateur.
6. Artifacts utilisateur : Velociraptor peut collecter des informations sur les utilisateurs, y compris les comptes d'utilisateurs, les appartennances à des groupes et l'historique de connexion.

Nous travail (Scénario)

l'artifact que j'utiliserai dans Velociraptor est l'artifact de processus. Cet artifact fournit des informations sur les processus en cours d'exécution sur le système cible, y compris les listes de processus, les arguments de ligne de commande et les bibliothèques chargées. Ces informations peuvent être extrêmement précieuses pour diverses enquêtes, telles que la détection et la réponse aux logiciels malveillants, la compromission du système et la réponse générale aux incidents. En analysant les informations de processus, vous pouvez mieux comprendre l'état du système et toute activité suspecte. Par exemple, si vous enquêtez sur une infection potentielle par un logiciel malveillant, vous pouvez utiliser les informations de processus pour identifier et isoler tout processus malveillant et effectuer une analyse plus approfondie de son comportement.

1 - Windows.Forensics.ProcessInfo

nous sélectionnons les artefacts Windows.Forensics.ProcessInfo

process.windows	Windows.Forensics.ProcessInfo								
Generic.System.Pstree	Type: client								
Windows.Attack.ParentProcess									
Windows.Detection.ForwardedImports	Extract information about processes.								
Windows.Detection.Yara.Process									
Windows.EventLogs.Evtx									
Windows.Forensics.ProcessInfo	Parameters								
Windows.NTFS.MFT	<table><thead><tr><th>Name</th><th>Type</th><th>Default</th><th>Description</th></tr></thead><tbody><tr><td>ProcessNameRegex</td><td>regex</td><td>^.</td><td></td></tr></tbody></table>	Name	Type	Default	Description	ProcessNameRegex	regex	^.	
Name	Type	Default	Description						
ProcessNameRegex	regex	^.							
Windows.Persistence.Debug									
Windows.Remediation.Sinkhole									
Windows.System.Amcache	Source								
Windows.System.SVCHost									
Windows.System.UntrustedBinaries									
Windows.System.VAD									
Windows.Triage.ProcessMemory									

Maintenant, nous commençons à chasser les résultats arrivent rapidement 1s

smss.exe	0x1a7fdb7000	352			▶ 0
csrss.exe	0xbaf6623000	436			▶ 0
csrss.exe	0x586e972000	512			▶ 0
wininit.exe	0xd0a843d000	520			▶ 0
winlogon.exe	0xeaa5ff3000	588	C:\Windows\system32	winlogon.exe	G:\Windows\system32
			\winlogon.exe		
					{ "ALLUSERSPROFILE": "C:\ProgramData", "CommonProgramFiles": "C:\Program Files\Common Files", "CommonProgramFiles(x86)": "C:\Program Files (x86)\Common Files", "CommonProgramW6432": "C:\Program Files\Common Files", "COMPUTERNAME": "PC-STATIAIRE", "ComSpec": "C:\Windows\system32\cmd.exe", "DriverData": "C:\Windows\System32\Drivers\DriverData", "NUMBER_OF_PROCESSORS": "2", "OS": "Windows_NT", "Path": "C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0;\...", "PATHEXT": ".COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC", "PROCESSOR_ARCHITECTURE": "AMD64", "PROCESSOR_IDENTIFIER": "Intel(R) Family 6 Model 15B Stepping 10, GenuineIntel", "PROCESSOR_LEVEL": "6", "PROCESSOR_REVISION": "9e0a", "ProgramData": "C:\ProgramData", "ProgramFiles": "C:\Program Files", "ProgramFiles(x86)": "C:\Program Files (x86)", "ProgramW6432": "C:\Program Files", "PSModulePath": "%ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32 }

Vous pouvez installer le fichier JSON

2 - Linux.Sys.LogHunter

L'artifact que j'utiliserais dans Velociraptor est l'artifact de processus. Cet artifact fournit des informations sur les processus en cours d'exécution sur comportement.

nous sélectionnons les artefacts Linux.Sys.LogHunter

Create Hunt: Select artifacts to collect

log windows

Linux.Sys.LogHunter

Windows.Applications.IISLogs

Windows.EventLogs.AlternateLogon

Windows.EventLogs.Cleared

Windows.EventLogs.DHCP

Windows.EventLogs.Evtx

Windows.EventLogs.EvtxHunter

Windows.EventLogs.ExplicitLogon

Windows.EventLogs.Kerberosing

Windows.EventLogs.Modifications

Windows.EventLogs.PowerShellModule

Windows.EventLogs.PowershellScriptblock

Windows.EventLogs.RDPAuth

Windows.Applications.IISLogs

Type: client

Author: Matt Green - @mgreen27

This artifact enables grep of IISLogs. Parameters include SearchRegex and WhitelistRegex as regex terms.

Parameters

Name	Type	Default	Description
IISLogFile	string	*/inpub/logs/*3/.log	
SearchRegex	regex	POST	Regex of strings to search in line.
WhitelistRegex	regex		Regex of strings to leave out of output.

Source

```
1 LET files = SELECTFullPath FROM glob(globs=IISLogFile)
2
3 SELECT * FROM foreach(row=files,
```

Configure Hunt

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

Active Windows

Maintenant, nous commençons à chasser les résultats arrivent rapidement 1s

Artifact Collection	Uploaded Files	Requests	Results	Log	Notebook
Overview					
Artifact Names	Linux.Sys.LogHunter				
Flow ID	F.CFJ213CFA0LA4				
Creator	H.CFJ2HRR0IS1S6				
Create Time	2023-02-10T11:22:53Z				
Start Time					
Last Active					
Duration	Running...				
State	RUNNING				
Ops/Sec	Unlimited				
CPU Limit	Unlimited				

Voici le fichier journal que nous collectons à partir du client Ubuntu

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.CFJ213FU7HU7M	Windows.Applications.IISLogs	2023-02-10T11:22:53Z	2023-02-10T11:24:13Z	H.CFJ0PNL4BPHU		
✓	F.CFJ213CFQA1LA4	Linux.Sys.LogHunter	2023-02-10T11:22:53Z	2023-02-10T11:24:14Z	H.CFJ2HRRRBS156		1
✓	F.CFJ213APCP2K8	Windows.Forensics.ProcessInfo	2023-02-10T11:22:53Z	2023-02-10T11:24:12Z	H.CFJ29252CKDK		318
✓	F.CFJ213ABVGNOQM	Windows.Applications.IISLogs	2023-02-10T11:22:53Z	2023-02-10T11:24:13Z	H.CFJ2F6D617U4B		
✓	F.CFJ213ABVGNOQM	Windows.Applications.IISLogs	2023-02-10T11:22:53Z	2023-02-10T11:24:13Z	H.CFJ2F6D617U4B		

Artifact Collection Uploaded Files Requests Results Log Notebook

Linux.Sys.LogHunter

OSPath Line

```
/var/log Jan 20 10:24:10 johan-virtual-machine snapd[1776]: taskrunner.go:289: [change 3 "Handling re-refresh of \"core\", \"core20\", \"gnome-3-38-2004\", \"gtk-common-themes\", \"snap-store\" as needed".task] failed: Post https://api.snapcraft.io/v2/snaps/refresh: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
```

10 25 50 Showing 1 to 1 of 1

* * * Data Page

Conclusion

En conclusion, la criminalistique numérique est un élément essentiel de la lutte contre la cybercriminalité et de la protection des informations sensibles. Il s'agit d'un domaine complexe et multidisciplinaire qui nécessite une compréhension approfondie de la technologie numérique, ainsi que l'utilisation d'outils et de techniques spécialisés. Alors que l'utilisation des appareils numériques continue de croître, la criminalistique numérique deviendra un domaine de plus en plus important dans les années à venir.