Evidence Preservation and Analysis

1. Objective

This report contains the details of the task including Volatile Data Collection, and Evidence Collection. The goal of this task is to:

- Learn evidence preservation and also analysis of evidence.

2. Introduction

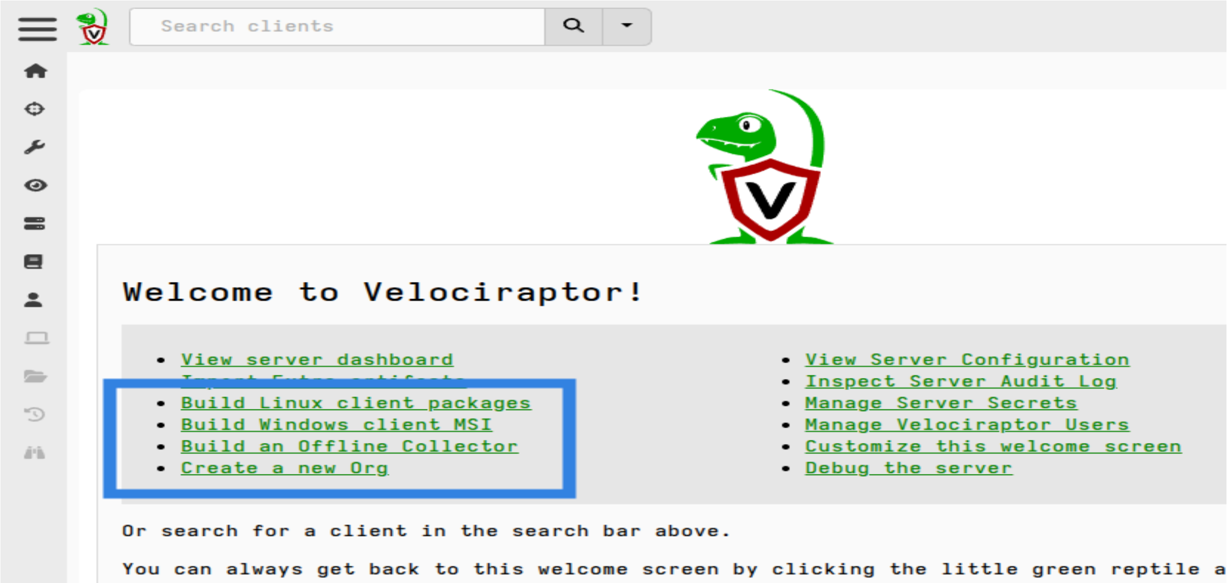
Evidence preservation and analysis is a digital forensic process for performing Investigation it involves collection of evidence, preservation of evidence, and analyzing the evidence to know the attackers tactics, and techniques. Performing further legal proceedings.

3. Tools

- Velociraptor setup using its official documentation. https://docs.velociraptor.app/downloads/
- FTK Imager is a forensic tool kit setup using exterro website. https://www.exterro.com/digital-forensics-software/ftk-imager

4. Volatile Data Collection

Volatile data collection is a process of collecting data from the computer only when it is running . That means it not collect data when the system is in off mode. Usually it collects data from RAM, Cache memory, network connections, and user activity.



Welcome to Velociraptor!

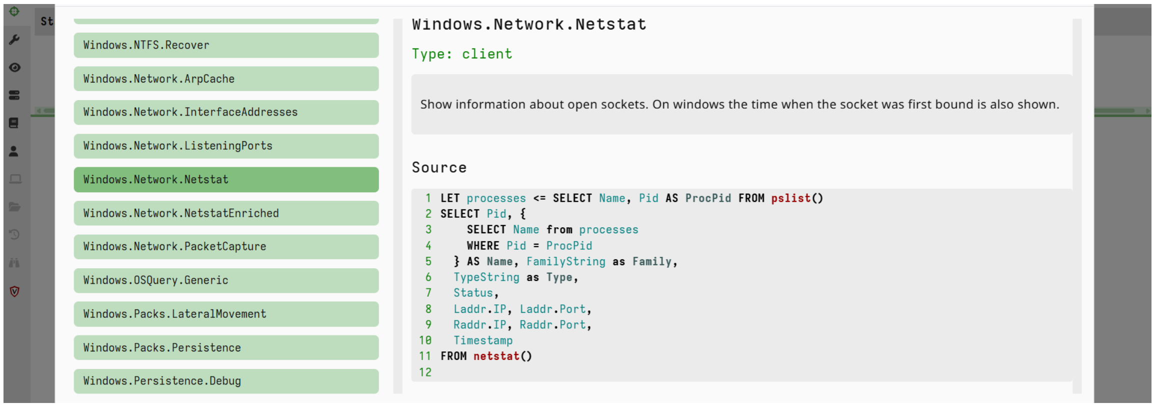
- View server dashboard
- Import Extra artifacts
- Build Linux client packages
- Build Windows client MSI
- Build an Offline Collector
- Create a new Org

- View Server Configuration
- Inspect Server Audit Log
- Manage Server Secrets
- Manage Velociraptor Users
- Customize this welcome screen
- Debug the server

Or search for a client in the search bar above.

You can always get back to this welcome screen by clicking the little green reptile a

Using Velociraptor for collecting network connections (SELECT * FROM Artifacts. Windows VM. saving it as CSV file.


St
Windows.NTFS.Recover
Windows.Network.ArpCache
Windows.Network.InterfaceAddresses
Windows.Network.ListeningPorts
Windows.Network.Netstat
Windows.Network.NetstatEnriched
Windows.Network.PacketCapture
Windows.OSQuery.Generic
Windows.Packs.LateralMovement
Windows.Packs.Persistence
Windows.Persistence.Debug

Windows.Network.Netstat

Type: client

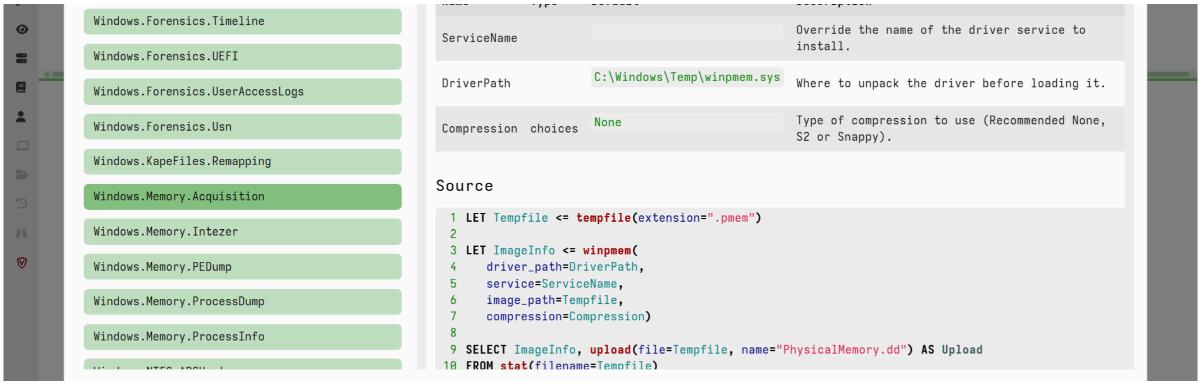
Show information about open sockets. On windows the time when the socket was first bound is also shown.

Source

```
LET processes <= SELECT Name, Pid AS ProcPid FROM pslist()
SELECT Pid, {
    SELECT Name from processes
    WHERE Pid = ProcPid
  } AS Name, FamilyString as Family,
  TypeString as Type,
  Status,
  Laddr.IP, Laddr.Port,
  Raddr.IP, Raddr.Port,
  Timestamp
FROM netstat()

```

5. Evidence Collection

Evidence collection is a crucial process of gathering and preserving the digital data from different sources to investigate incidents and to support legal proceedings. Collecting a Memory dump (SELECT* FROM Artifact.Windows.memory.Acquisition) and hash it Using sha256sum.


Windows.Forensics.Timeline
Windows.Forensics.UEFI
Windows.Forensics.UserAccessLogs
Windows.Forensics.Usn
Windows.KapeFiles.Remapping
Windows.Memory.Acquisition
Windows.Memory.Intezer
Windows.Memory.PEDump
Windows.Memory.ProcessDump
Windows.Memory.ProcessInfo

ServiceName			Override the name of the driver service to install.
DriverPath		C:\Windows\Temp\winpmem.sys	Where to unpack the driver before loading it.
Compression	choices	None	Type of compression to use (Recommended None, S2 or Snappy).

Source

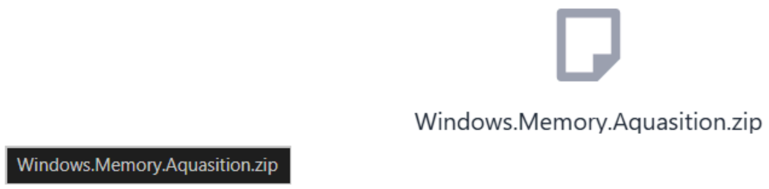
```
LET Tempfile <= tempfile(extension=".pmem")

LET ImageInfo <= winpmem(
   driver_path=DriverPath,
   service=ServiceName,
   image_path=Tempfile,
   compression=Compression)

SELECT ImageInfo, upload(file=Tempfile, name="PhysicalMemory.dd") AS Upload
FROM stat(filename=Tempfile)
```

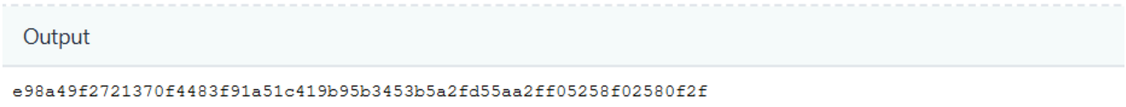
5.1 Collected Evidence metadata

Below table shows the metadata of evidence collected and it includes Item, Description, Collected BY, Date, and Hash Value.

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-Y Dump	SOC Analyst	2025-10-23	e98a49f2721370f4483f91a51c419b95b3453b5a2fd55aa2ff05258f02580f2f

The below image shows the hash value of the Windows.Memory.Aquasition file. That is taken from the Velociraptor tool. By performing the activity I collected data and that data I converted as a hash file.




Output

```
e98a49f2721370f4483f91a51c419b95b3453b5a2fd55aa2ff05258f02580f2f
```