OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

Michael Hegarty

Forensics

Extracting Volatile Data (Manually)

Contents

Extracting Volatile Data (Manually)

In forensic investigations, collecting volatile data is a crucial step. Volatile data refers to data stored in memory (RAM) that will be lost when the system is powered off or rebooted. Extracting this data as quickly as possible ensures that important evidence, such as running processes, open files, network connections, and more, is preserved.

In this exercise, we will use several **Command Line Interface (CLI)** commands to manually extract volatile data from a system. The following commands represent a common subset that forensic investigators often use. While this list is not exhaustive, it covers the essentials for gathering volatile data effectively.

What is Volatile Data?

In computer forensics, two main types of data are collected during an investigation: **persistent data** and **volatile data**.

1. **Persistent Data**:
   - Persistent data is stored on a local hard drive or non-volatile storage device (such as SSDs, external drives, USB sticks).
   - This data remains intact and is preserved even when the computer is powered off.
   - Examples include files, documents, images, system logs, and software installed on the hard drive.
2. **Volatile Data**:

- Volatile data, is any data stored in temporary memory locations such as the system's **random access memory (RAM)** or **cache**.
- This type of data is **lost when the computer is powered off** or rebooted, making it time-sensitive and crucial to capture during a live forensic investigation.
- Volatile data contains critical information like running processes, open network connections, active user sessions, encryption keys, and other ephemeral data.

Importance of Volatile Data in Forensic Investigations

Volatile data is invaluable in forensic investigations, particularly when investigating active incidents like malware attacks or unauthorized access. Since volatile data exists in RAM and the system's active memory, it captures information about what is happening on the machine in real-time. This information may include:

- **Running processes and programs**: Helps investigators identify malicious programs or services.
- **Network connections**: Useful for detecting active or past connections to external systems, which may indicate data exfiltration or other malicious activities.
- **Open files and registry information**: Shows files currently in use, and can indicate tampering or unauthorized access.
- **Login sessions and user activity**: Can help in identifying unauthorized access or intrusions.

Live Forensics

The process of capturing and analysing volatile data while the system is still running is known as **live forensics**. This type of investigation requires careful handling to avoid altering the volatile data during collection. Investigators use specialized tools to capture a "snapshot" of the system's current volatile data without shutting down the system.

The challenge with volatile data is that it is fleeting. If the system is powered off, rebooted, or crashes, all volatile data is irreversibly lost. Therefore, in incident response situations, collecting volatile data is often the **priority** before further steps, such as disk imaging, are taken.

Understanding and capturing volatile data is essential to gaining insights into ongoing security threats and determining how a system was compromised.

System Information

The **System Information** tool in Windows provides detailed diagnostic and troubleshooting information about a system's **operating system, hardware, and software**. This tool is often used in forensic investigations to capture essential volatile data, offering insights into the system's current state.

Capturing System Information via Command Line

In live forensic investigations, collecting system data is crucial for analysis. One method to gather this volatile data is by using command-line tools. Specifically, the **systeminfo** command is used to obtain detailed information about the system, such as:

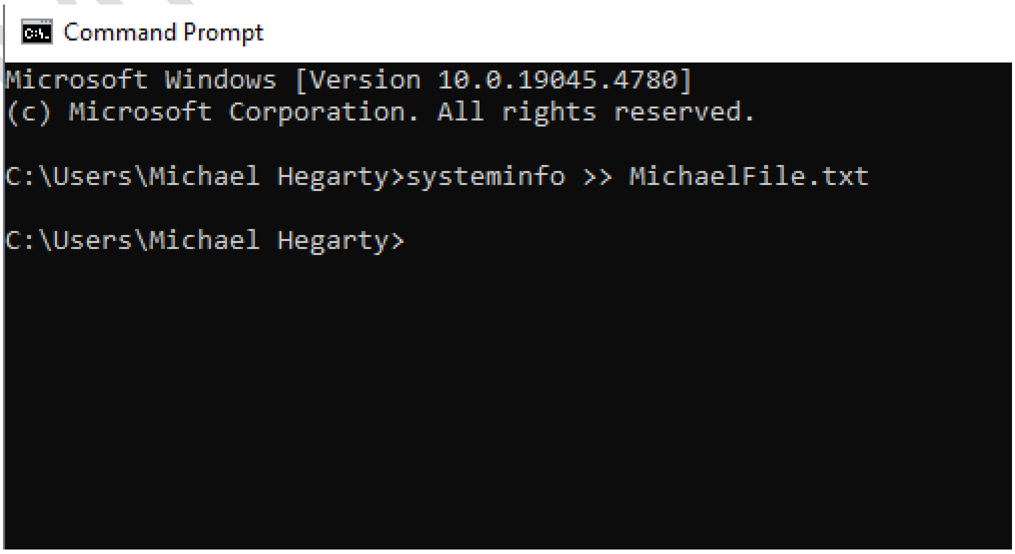
- **Operating System Version**
- **Processor Information**
- **Memory Usage**
- **Network Configuration**
- **System Boot Time**
- **Patch/Update Details**

Command to Capture System Information:

To capture the system information and save it into a text file for later analysis, follow these steps:

1. Open the **Command Prompt** as an Administrator.
2. Type the following command to extract system information and save it into a file named MichaelFile.txt:

systeminfo >> MichaelFile.txt

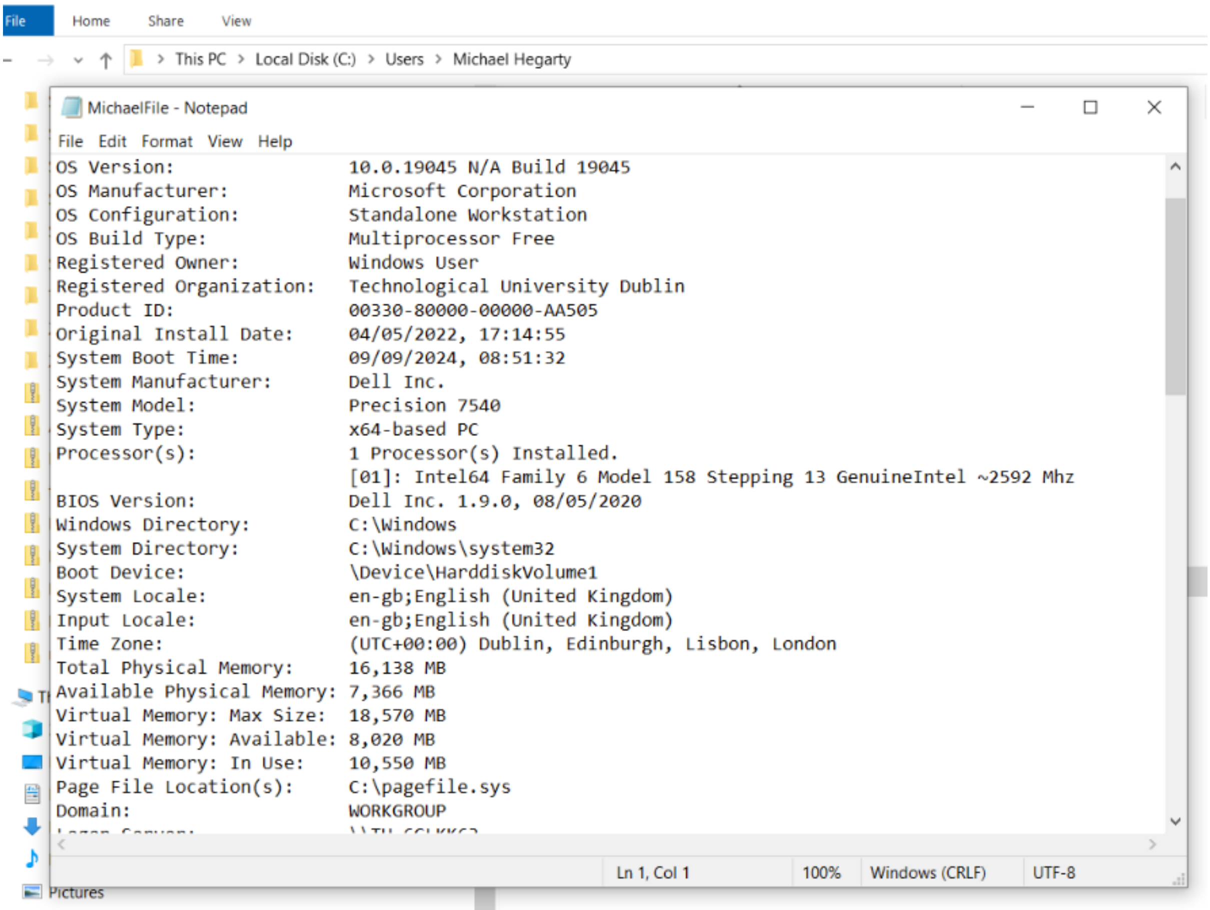


```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Michael Hegarty>systeminfo >> MichaelFile.txt

C:\Users\Michael Hegarty>
```

Now, go to this location to see the results of this command. Where it will show all the system information about your system software and hardware.



```
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:   Technological University Dublin
Product ID:                00330-80000-00000-AA505
Original Install Date:     04/05/2022, 17:14:55
System Boot Time:          09/09/2024, 08:51:32
System Manufacturer:       Dell Inc.
System Model:              Precision 7540
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 13 GenuineIntel ~2592 Mhz
BIOS Version:              Dell Inc. 1.9.0, 08/05/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     16,138 MB
Available Physical Memory: 7,366 MB
Virtual Memory: Max Size:  18,570 MB
Virtual Memory: Available: 8,020 MB
Virtual Memory: In Use:    10,550 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```

Why Use the systeminfo Command in Forensics?

- **Documentation of System State**: The systeminfo command provides an essential snapshot of the system’s current configuration.
- **Tracking System Changes**: By comparing the results before and after certain events (such as suspected breaches), forensic investigators can detect discrepancies.
- **Log Collection**: This data is preserved in a text file, which can later be analyzed or shared with a forensic team for further investigation.

Currently Available Network Connections

Network connectivity refers to the process of connecting different devices and systems through routers, switches, and gateways to enable communication within a network. During forensic investigations, analysing current network connections helps in identifying active connections, potential threats, or unauthorized communication.

Checking Active Network Connections via Command Line

Using the **netstat** (network statistics) command, we can capture details about all active network connections, including:

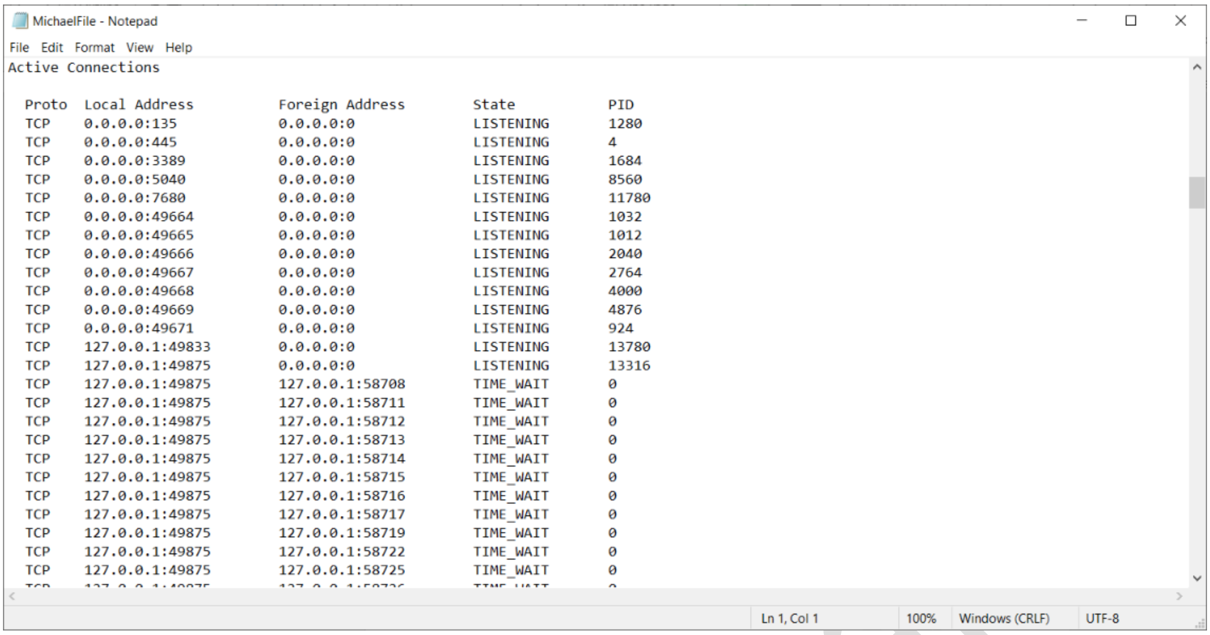
- **Protocol** (TCP/UDP)
- **Local and Remote Addresses**
- **Port Numbers**
- **Connection State** (e.g., Established, Listening)
- **Process ID (PID)** of the application responsible for the connection

This information is vital in forensic investigations to determine if there are any suspicious or unauthorized connections on a system.

We can check all the currently available network connections through the command line.

```
netstat -nao >> MichaelFile.txt
```

Now, open that text file to see all active connections in the system right now. It will also provide us with some extra details like state, PID, address, protocol.



```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1280
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1684
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8560
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       11780
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1032
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1012
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2040
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2764
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       4000
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       4876
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       924
  TCP    127.0.0.1:49833        0.0.0.0:0              LISTENING       13780
  TCP    127.0.0.1:49875        0.0.0.0:0              LISTENING       13316
  TCP    127.0.0.1:49875        127.0.0.1:58708        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58711        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58712        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58713        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58714        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58715        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58716        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58717        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58719        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58722        TIME_WAIT       0
  TCP    127.0.0.1:49875        127.0.0.1:58725        TIME_WAIT       0
```

Routing Configuration in Forensic Investigation

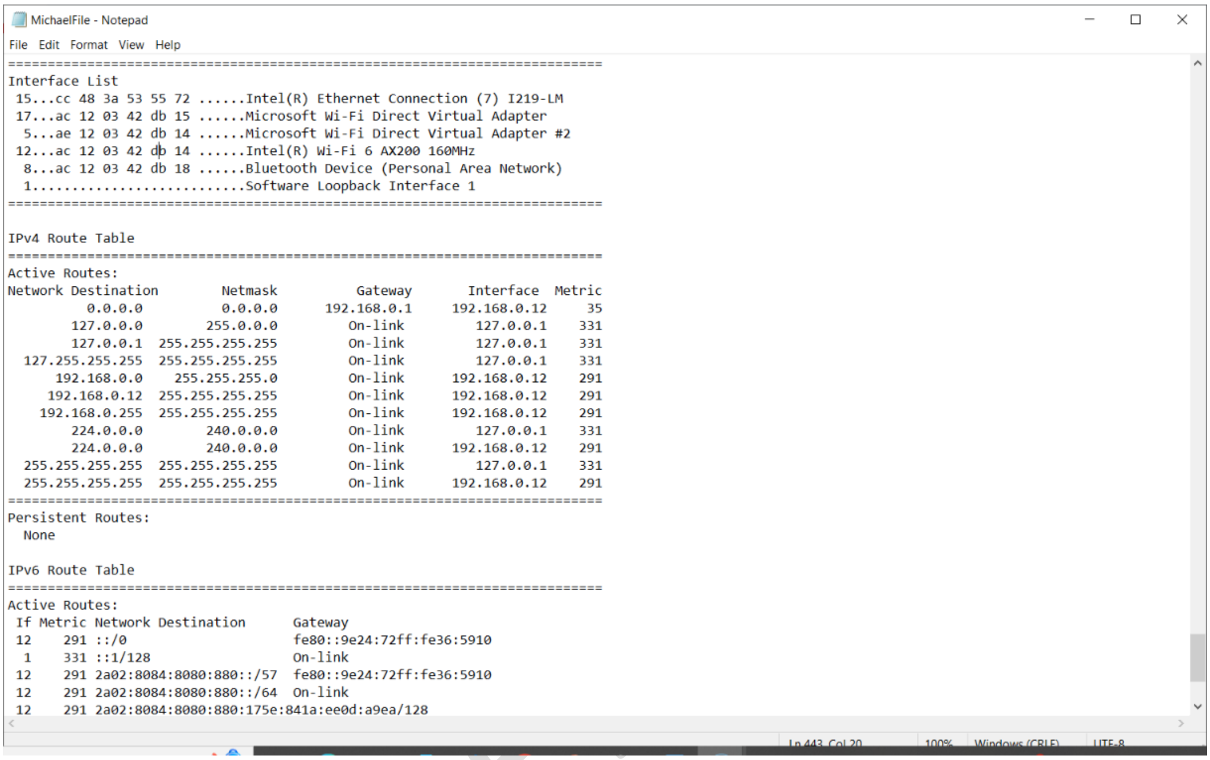
Routing configuration refers to the setup of IP addresses, gateway settings, and network routes that direct data traffic between devices in a network. This information is crucial in digital forensics because improper or malicious routing could indicate unauthorized access or a compromised system.

Importance of Routing Configuration in Forensics:

- **Network Traffic Analysis**: Routing configuration helps investigators understand how data travels within a network, which is essential for detecting anomalies, such as unauthorized external connections or traffic being rerouted through malicious servers.
- **Identifying Potential Threats**: Misconfigured or altered routing tables can be a sign of network hijacking or man-in-the-middle attacks, where attackers intercept and manipulate network traffic.

To know the Router configuration in our network follows this command.

route print >> MichaelFile.txt



```
===========================================================================
Interface List
 15...cc 48 3a 53 55 72 ......Intel(R) Ethernet Connection (7) I219-LM
 17...ac 12 03 42 db 15 ......Microsoft Wi-Fi Direct Virtual Adapter
  5...ae 12 03 42 db 14 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 12...ac 12 03 42 db 14 ......Intel(R) Wi-Fi 6 AX200 160MHz
  8...ac 12 03 42 db 18 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1     192.168.0.12     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link      192.168.0.12    291
     192.168.0.12  255.255.255.255         On-link      192.168.0.12    291
    192.168.0.255  255.255.255.255         On-link      192.168.0.12    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.0.12    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.0.12    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 12    291 ::/0                     fe80::9e24:72ff:fe36:5910
  1    331 ::1/128                  On-link
 12    291 2a02:8084:8080:880::/57  fe80::9e24:72ff:fe36:5910
 12    291 2a02:8084:8080:880::/64  On-link
 12    291 2a02:8084:8080:880:175e:841a:ee0d:a9ea/128
```

Why Routing and Host Configuration Matter in Forensics:

1. **Identifying Misconfigured Routes**: If routes are misconfigured or if there are unknown routes in the routing table, this could point to unauthorized access or malicious redirection of traffic.
2. **Understanding Network Topology**: Analyzing the routing and host configuration helps map out how the network is set up and identify if attackers have modified these settings.

3. **Detecting Unauthorized Devices**: Reviewing IP configuration and gateway settings can help identify if there are any unauthorized devices attempting to reroute traffic or engage in suspicious network activities.

Please run the following commands on your machine.

Screenshot the results of your txt file (like the above)

Write a brief explanation of what each command is doing

Place your screenshots and explanations in a MS Word Document and upload to Brightspace by 8pm on Sunday

1 Date and Time

```
echo %date% %time% > MichaelFile.txt
```

2 System Variables

```
set >> MichaelFile.txt
```

3 Task List

```
tasklist >> MichaelFile.txt
```

4 Task List with Modules

```
tasklist /m >> MichaelFile.txt
```

5 Task List with Services

```
tasklist /svc >> MichaelFile.txt
```

6 Workstation Information

```
net config workstation >> MichaelFile.txt
```

7 MAC Address saved in System ARP Cache

```
arp -a >> MichaelFile.txt
```

8 DNS Configuration

```
ipconfig /displaydns >> MichaelFile.txt
```

9 System network shares

```
net share >> MichaelFile.txt
```

10 Network Configuration

```
ipconfig /all >> MichaelFile.txt
```