Fast Incident Response and Data Collection

October 11, 2020 By Raj Chandel

In this article, we will gather information utilizing the quick incident response tools which are recorded beneath. All these tools are a few of the greatest tools available freely online. Through these, you can enhance your Cyber Forensics skills.

Table of Contents

Introduction

Incident Response

- Incident response, organized strategy for taking care of security occurrences, breaks, and cyber attacks.
- IR plan permits you to viably recognize, limit the harm, and decrease the expense of a cyber attack while finding and fixing the reason to forestall future assaults.

Data Collection

- Data collection is the process to securely gather and safeguard your client's electronically stored information (ESI) from PCs, workstations, workers, cloud stores, email accounts, tablets, cell phones, or PDAs.

Proof of Concept

Live Response Collection-Cederpelta Build

Live Response Collection -cedarpelta, an automated live response tool, collects volatile data, and create a memory dump. .This tool is created by **BriMor Labs**.

You can download the tool from **here**.

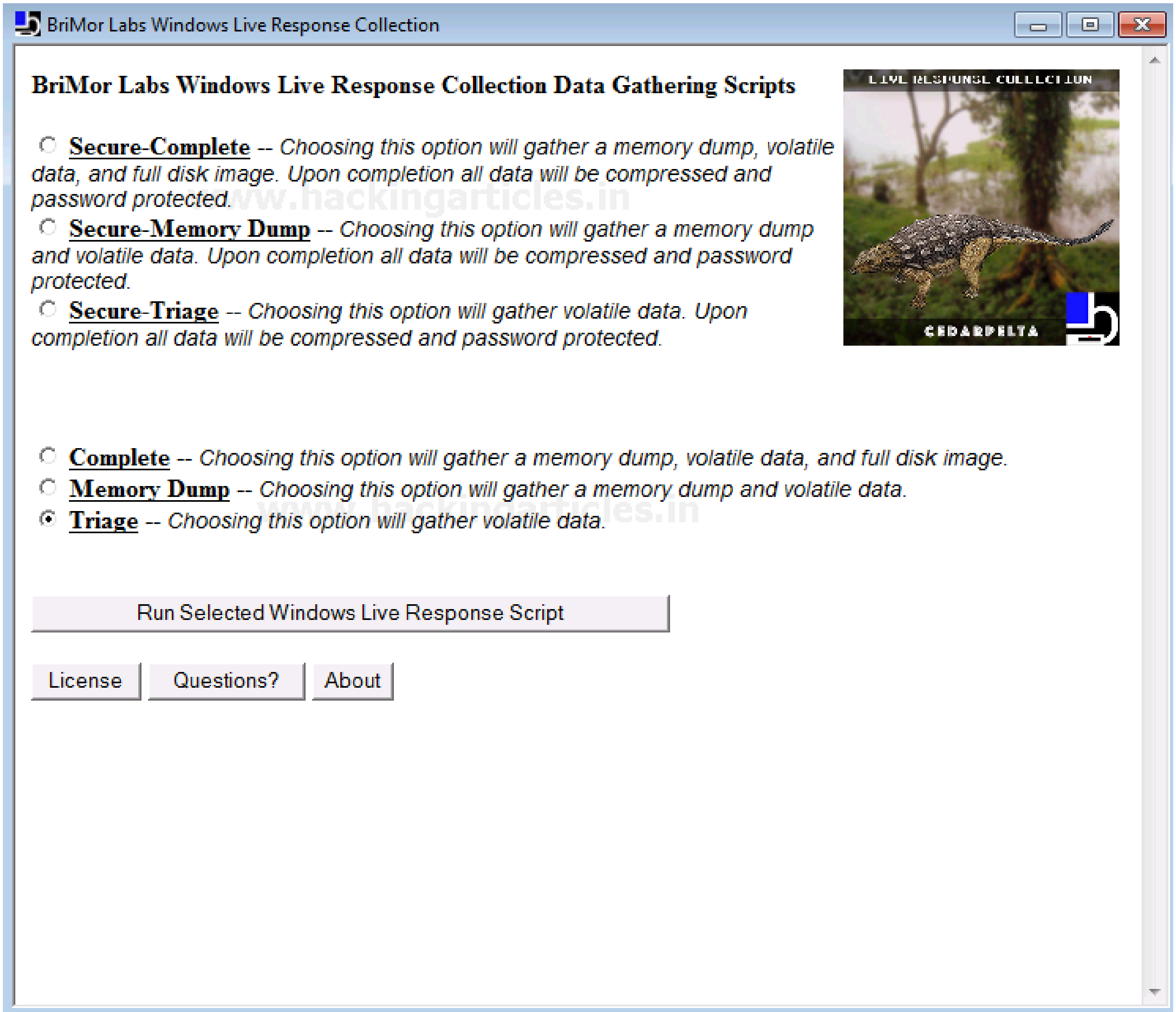
The live response is a zone that manages gathering data from a live machine to distinguish if an occurrence has happened. Such information incorporates artifacts, for example, process lists, connection information, files stored, registry information, etc.

It supports Windows, OSX/ mac OS, and *nix based operating systems. This instrument is kind of convenient to utilize on the grounds that it clarifies quickly which choice does what.

Let’s begin by exploring how the tool works:

The live response collection can be done by the following data gathering scripts

- Secure-Complete: Picking this choice will create a memory dump, collects volatile information, and also creates a full disk image. All the information collected will be compressed and protected by a password.
- Secure-Memory Dump: Picking this choice will create a memory dump and collects volatile data. All the information collected will be compressed and protected by a password.
- Secure- Triage: Picking this choice will only collect volatile data. All the information collected will be compressed and protected by a password.
- Complete: Picking this choice will create a memory dump, collects volatile information, and also creates a full disk image.
- Memory dump: Picking this choice will create a memory dump and collects volatile data.
- Triage: Picking this choice will only collect volatile data.



BriMor Labs Windows Live Response Collection Data Gathering Scripts

○ **Secure-Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image. Upon completion all data will be compressed and password protected.*

○ **Secure-Memory Dump** -- *Choosing this option will gather a memory dump and volatile data. Upon completion all data will be compressed and password protected.*

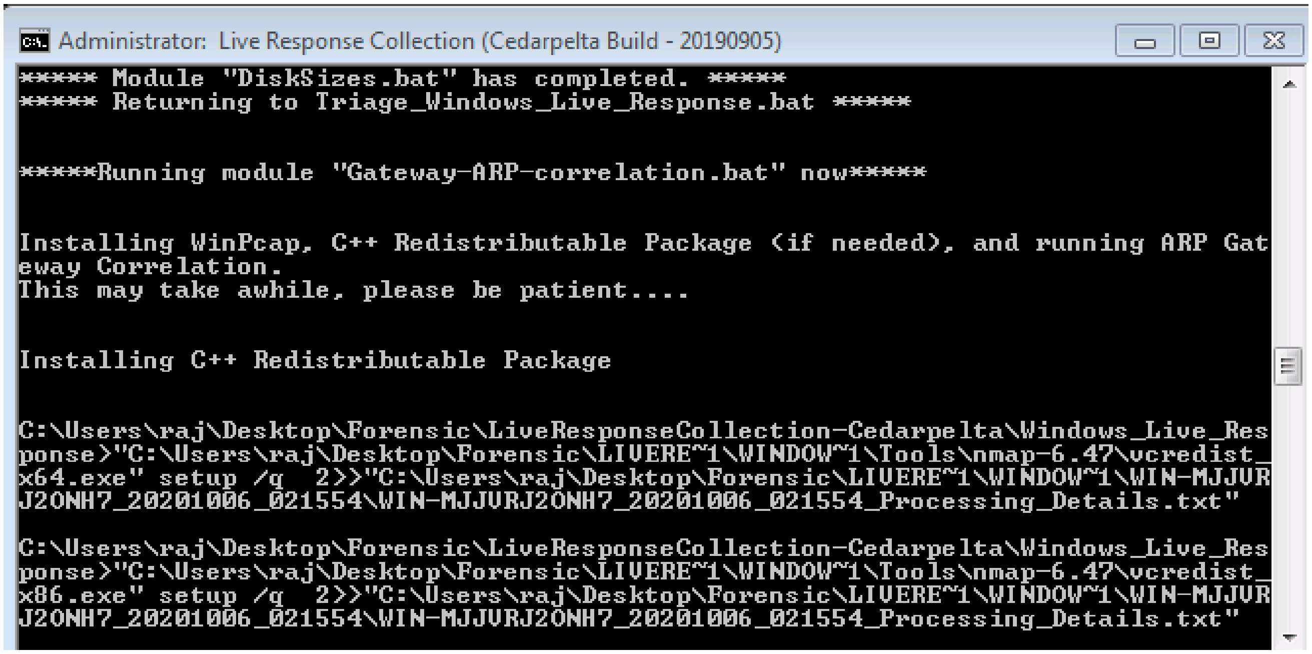
○ **Secure-Triage** -- *Choosing this option will gather volatile data. Upon completion all data will be compressed and password protected.*

○ **Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image.*

○ **Memory Dump** -- *Choosing this option will gather a memory dump and volatile data.*

● **Triage** -- *Choosing this option will gather volatile data.*

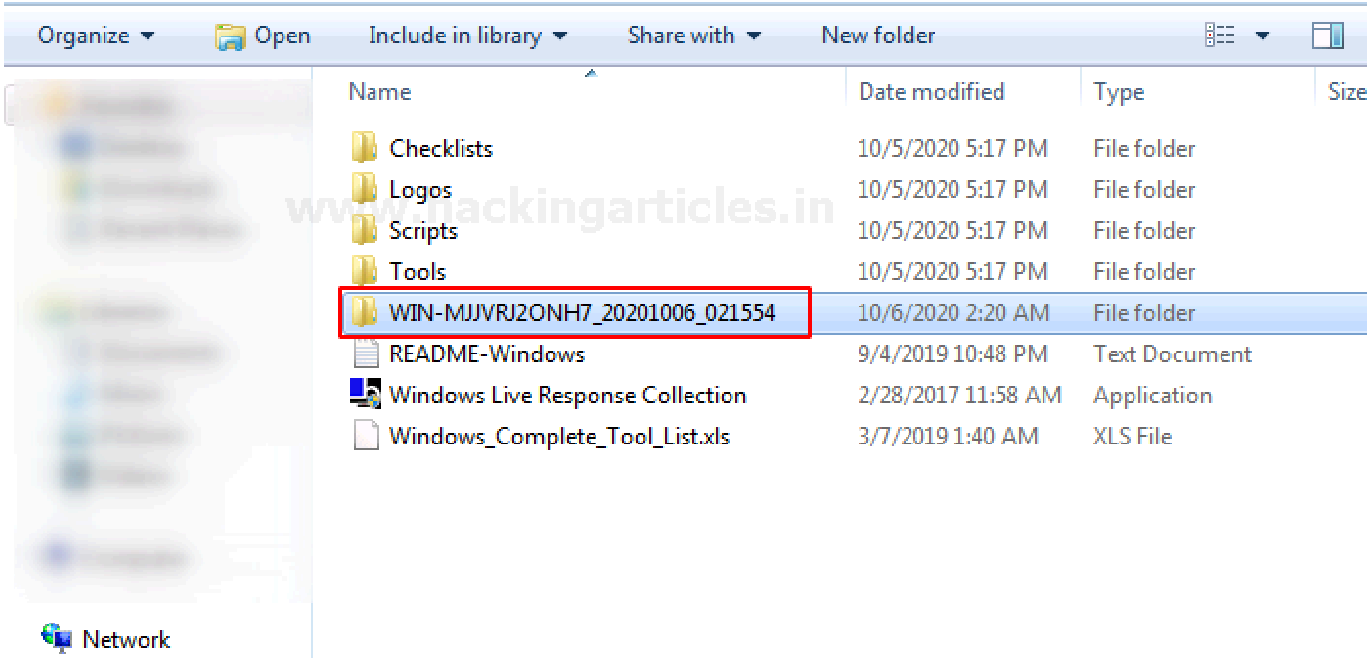
The process of data collection will begin soon after you decide on the above options. This might take a couple of minutes.



Administrator: Live Response Collection (Cedarpelta Build - 20190905)

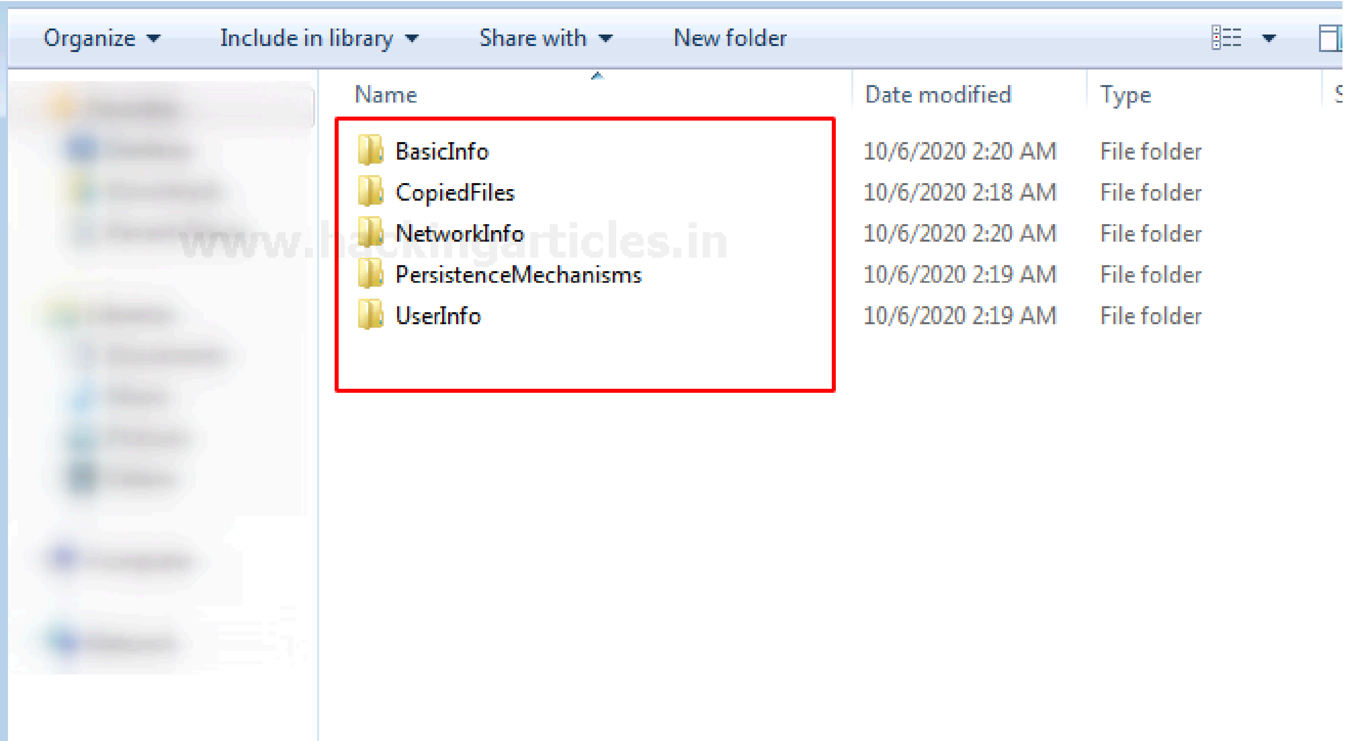
```
***** Module "DiskSizes.bat" has completed. *****
***** Returning to Triage_Windows_Live_Response.bat *****


*****Running module "Gateway-ARP-correlation.bat" now*****


Installing WinPcap, C++ Redistributable Package (if needed), and running ARP Gat
eway Correlation.
This may take awhile, please be patient....


Installing C++ Redistributable Package


C:\Users\raj\Desktop\Forensic\LiveResponseCollection-Cedarpelta\Windows_Live_Res
ponse>"C:\Users\raj\Desktop\Forensic\LIVERE~1\WINDOW~1\Tools\nmap-6.47\vcredist_
x64.exe" setup /q  2>>"C:\Users\raj\Desktop\Forensic\LIVERE~1\WINDOW~1\WIN-MJJVR
J2ONH7_20201006_021554\WIN-MJJVRJ2ONH7_20201006_021554_Processing_Details.txt"

C:\Users\raj\Desktop\Forensic\LiveResponseCollection-Cedarpelta\Windows_Live_Res
ponse>"C:\Users\raj\Desktop\Forensic\LIVERE~1\WINDOW~1\Tools\nmap-6.47\vcredist_
x86.exe" setup /q  2>>"C:\Users\raj\Desktop\Forensic\LIVERE~1\WINDOW~1\WIN-MJJVR
J2ONH7_20201006_021554\WIN-MJJVRJ2ONH7_20201006_021554_Processing_Details.txt"
```

After, the process is over it creates an output folder with the name of your computer alongside the date at the same destination where the executable file is stored.



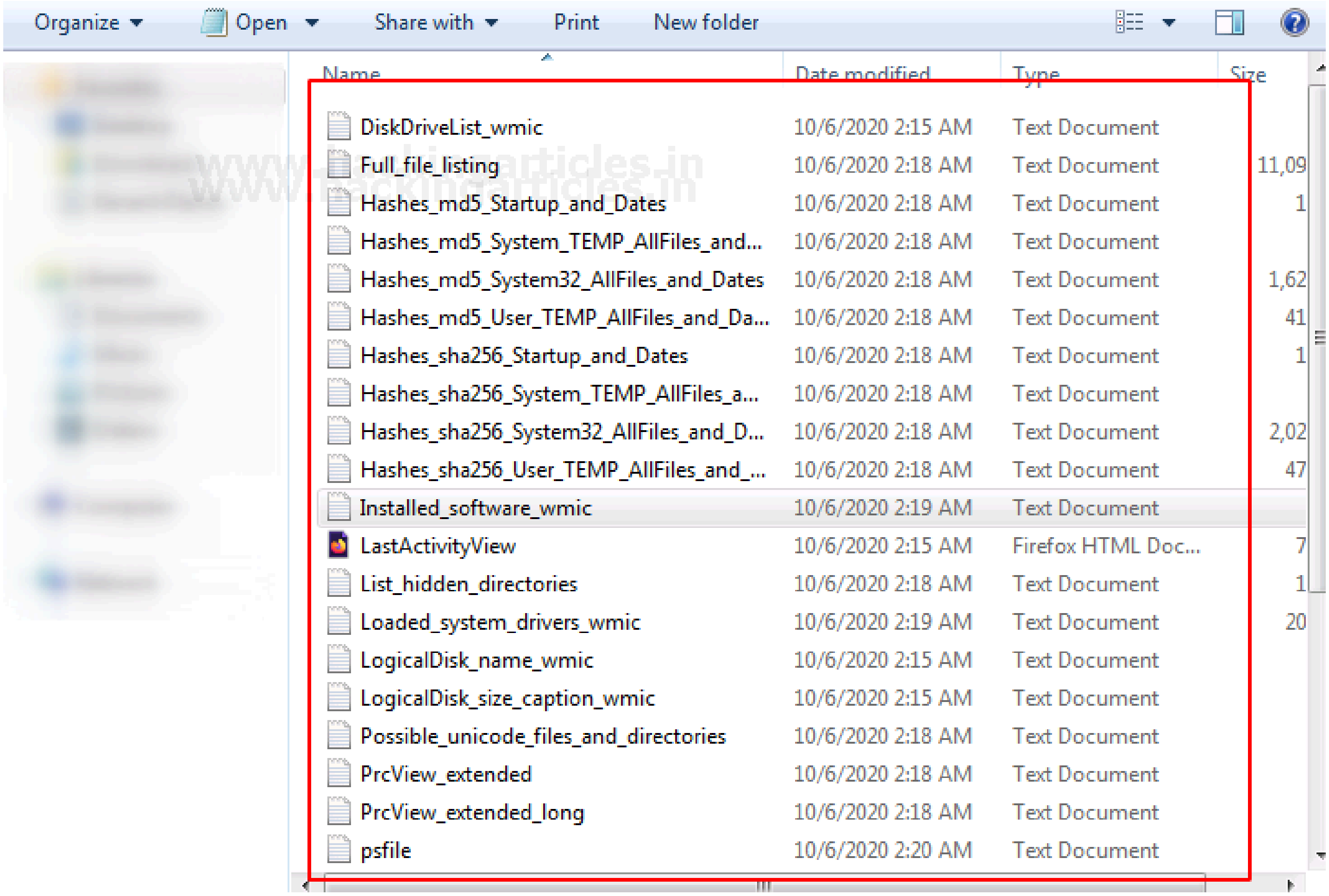
Name	Date modified	Type	Size
Checklists	10/5/2020 5:17 PM	File folder	
Logos	10/5/2020 5:17 PM	File folder	
Scripts	10/5/2020 5:17 PM	File folder	
Tools	10/5/2020 5:17 PM	File folder	
WIN-MJJVRJ2ONH7_20201006_021554	10/6/2020 2:20 AM	File folder	
README-Windows	9/4/2019 10:48 PM	Text Document	
Windows Live Response Collection	2/28/2017 11:58 AM	Application	
Windows_Complete_Tool_List.xls	3/7/2019 1:40 AM	XLS File	

The output folder consists of the following data segregated in different parts.



Name	Date modified	Type
BasicInfo	10/6/2020 2:20 AM	File folder
CopiedFiles	10/6/2020 2:18 AM	File folder
NetworkInfo	10/6/2020 2:20 AM	File folder
PersistenceMechanisms	10/6/2020 2:19 AM	File folder
UserInfo	10/6/2020 2:19 AM	File folder

These are few records gathered by the tool. You can check the individual folder according to your proof necessity. It collects RAM data, Network info, Basic system info, system files, user info, and much more.



Name	Date modified	Type	Size
DiskDriveList_wmic	10/6/2020 2:15 AM	Text Document	
Full_file_listing	10/6/2020 2:18 AM	Text Document	11,09
Hashes_md5_Startup_and_Dates	10/6/2020 2:18 AM	Text Document	1
Hashes_md5_System_TEMP_AllFiles_and...	10/6/2020 2:18 AM	Text Document	
Hashes_md5_System32_AllFiles_and_Dates	10/6/2020 2:18 AM	Text Document	1,62
Hashes_md5_User_TEMP_AllFiles_and_Da...	10/6/2020 2:18 AM	Text Document	41
Hashes_sha256_Startup_and_Dates	10/6/2020 2:18 AM	Text Document	1
Hashes_sha256_System_TEMP_AllFiles_a...	10/6/2020 2:18 AM	Text Document	
Hashes_sha256_System32_AllFiles_and_D...	10/6/2020 2:18 AM	Text Document	2,02
Hashes_sha256_User_TEMP_AllFiles_and_...	10/6/2020 2:18 AM	Text Document	47
Installed_software_wmic	10/6/2020 2:19 AM	Text Document	
LastActivityView	10/6/2020 2:15 AM	Firefox HTML Doc...	7
List_hidden_directories	10/6/2020 2:18 AM	Text Document	1
Loaded_system_drivers_wmic	10/6/2020 2:19 AM	Text Document	20
LogicalDisk_name_wmic	10/6/2020 2:15 AM	Text Document	
LogicalDisk_size_caption_wmic	10/6/2020 2:15 AM	Text Document	
Possible_unicode_files_and_directories	10/6/2020 2:18 AM	Text Document	
PrcView_extended	10/6/2020 2:18 AM	Text Document	
PrcView_extended_long	10/6/2020 2:18 AM	Text Document	
psfile	10/6/2020 2:20 AM	Text Document	

CDIR (Cyber Defense Institute Incident Response) Collector

CDIR (Cyber Defense Institute Incident Response) Collector is a data acquisition tool for the Windows operating system. The tool is created by Cyber Defense Institute, Tokyo Japan. The tool collects RAM, Registry data, NTFS data, Event logs, Web history, and many more.

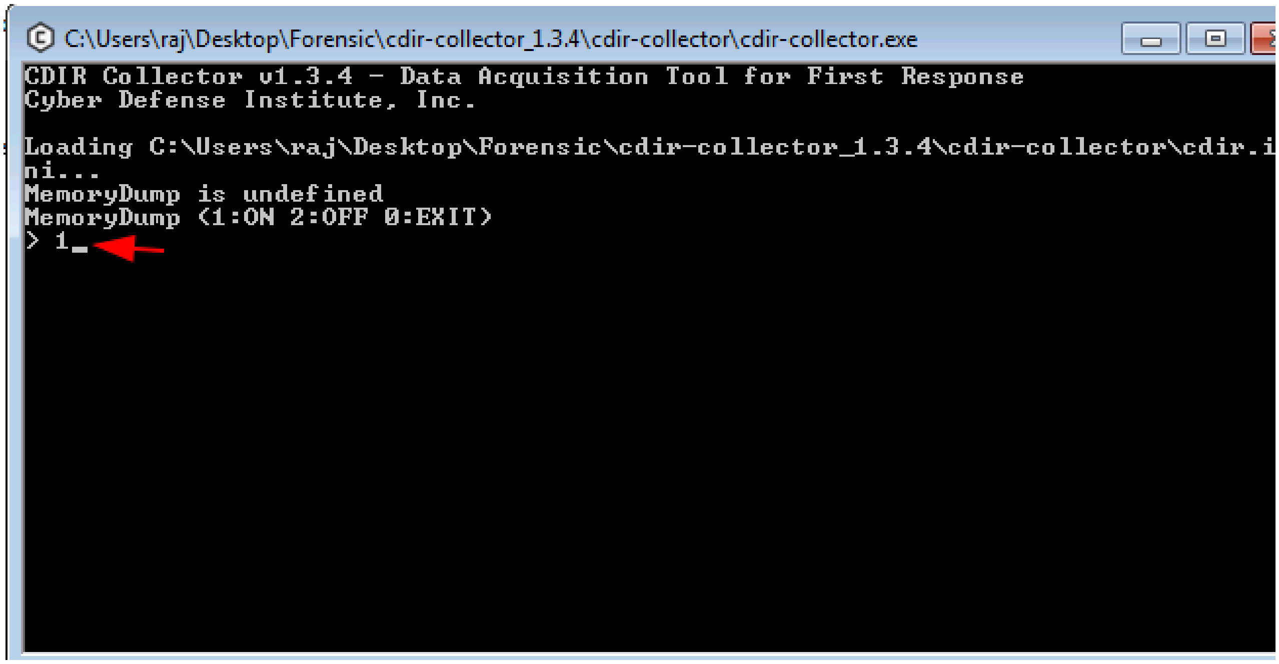
You can download the tool from **here**.

Let's begin by exploring how the tool works:

There are three options

1. To initiate the memory dump process (1: ON)
2. To stop the memory dump process and (2: OFF)
3. Exit (0: EXIT)

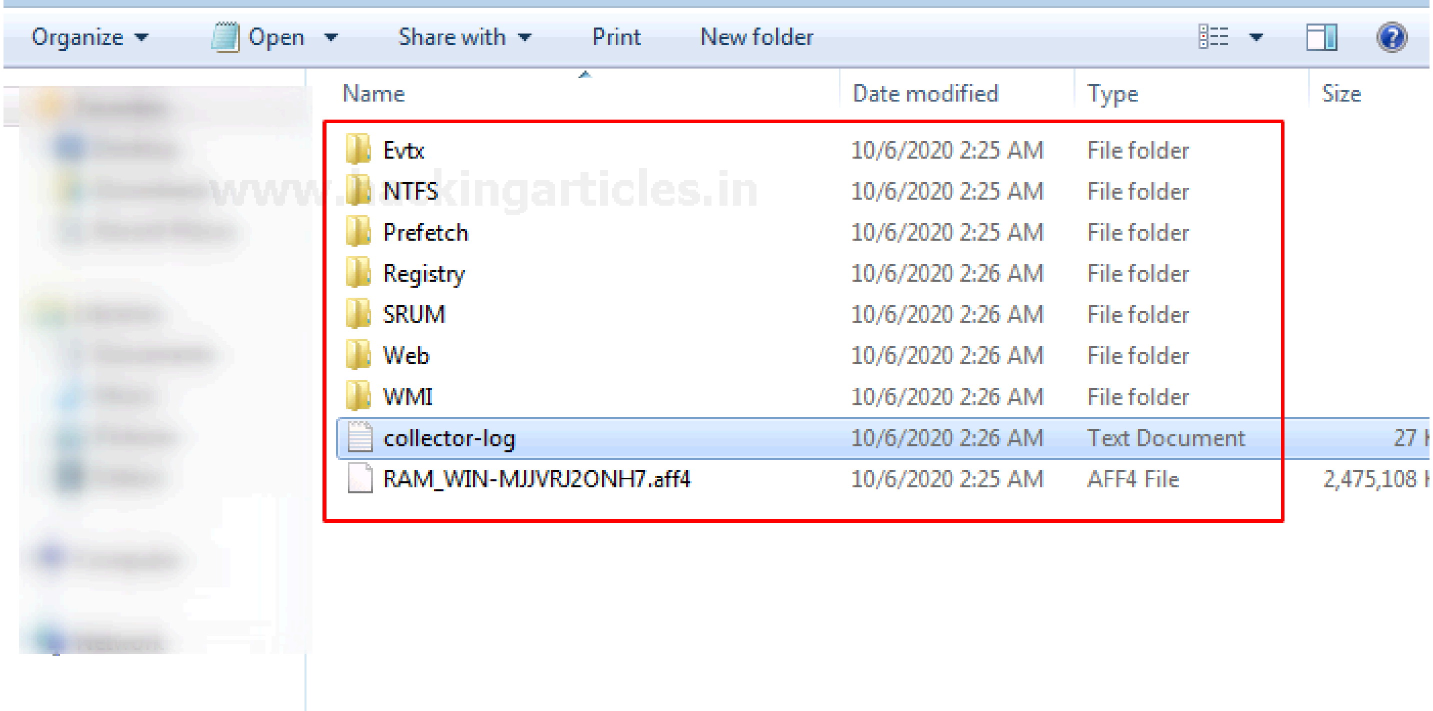
After successful installation of the tool, to create a memory dump select 1 that is to initiate the memory dump process (**1:ON**)



C:\Users\raj\Desktop\Forensic\cdir-collector_1.3.4\cdir-collector\cdir-collector.exe

```
CDIR Collector v1.3.4 - Data Acquisition Tool for First Response
Cyber Defense Institute, Inc.

Loading C:\Users\raj\Desktop\Forensic\cdir-collector_1.3.4\cdir-collector\cdir.i
ni...
MemoryDump is undefined
MemoryDump (1:ON 2:OFF 0:EXIT)
> 1_
```

Soon after the process is completed, an output folder is created with the name of your computer alongside the date at the same destination where the executable file is stored.



Name	Date modified	Type	Size
Evtx	10/6/2020 2:25 AM	File folder	
NTFS	10/6/2020 2:25 AM	File folder	
Prefetch	10/6/2020 2:25 AM	File folder	
Registry	10/6/2020 2:26 AM	File folder	
SRUM	10/6/2020 2:26 AM	File folder	
Web	10/6/2020 2:26 AM	File folder	
WMI	10/6/2020 2:26 AM	File folder	
collector-log	10/6/2020 2:26 AM	Text Document	27
RAM_WIN-MJJVRJ2ONH7.aff4	10/6/2020 2:25 AM	AFF4 File	2,475,108

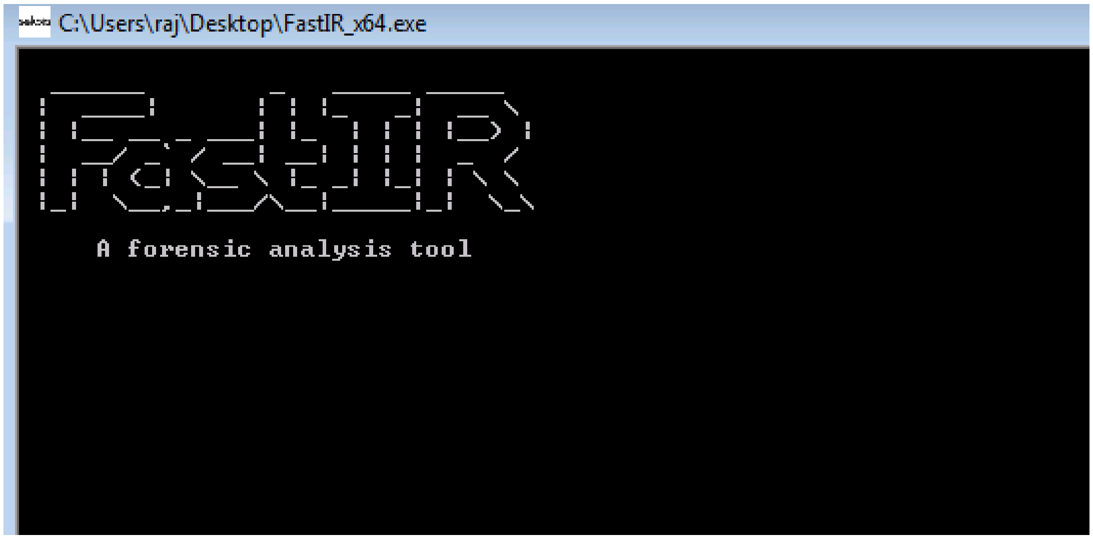
Fast IR Collector

Fast IR Collector is a forensic analysis tool for Windows and Linux OS. It gathers the artifacts from the live machine and records the yield in the .csv or .json document. Windows and Linux OS. This tool is created by ~~**SekoiaLab**~~.

You can download the tool from **here**.

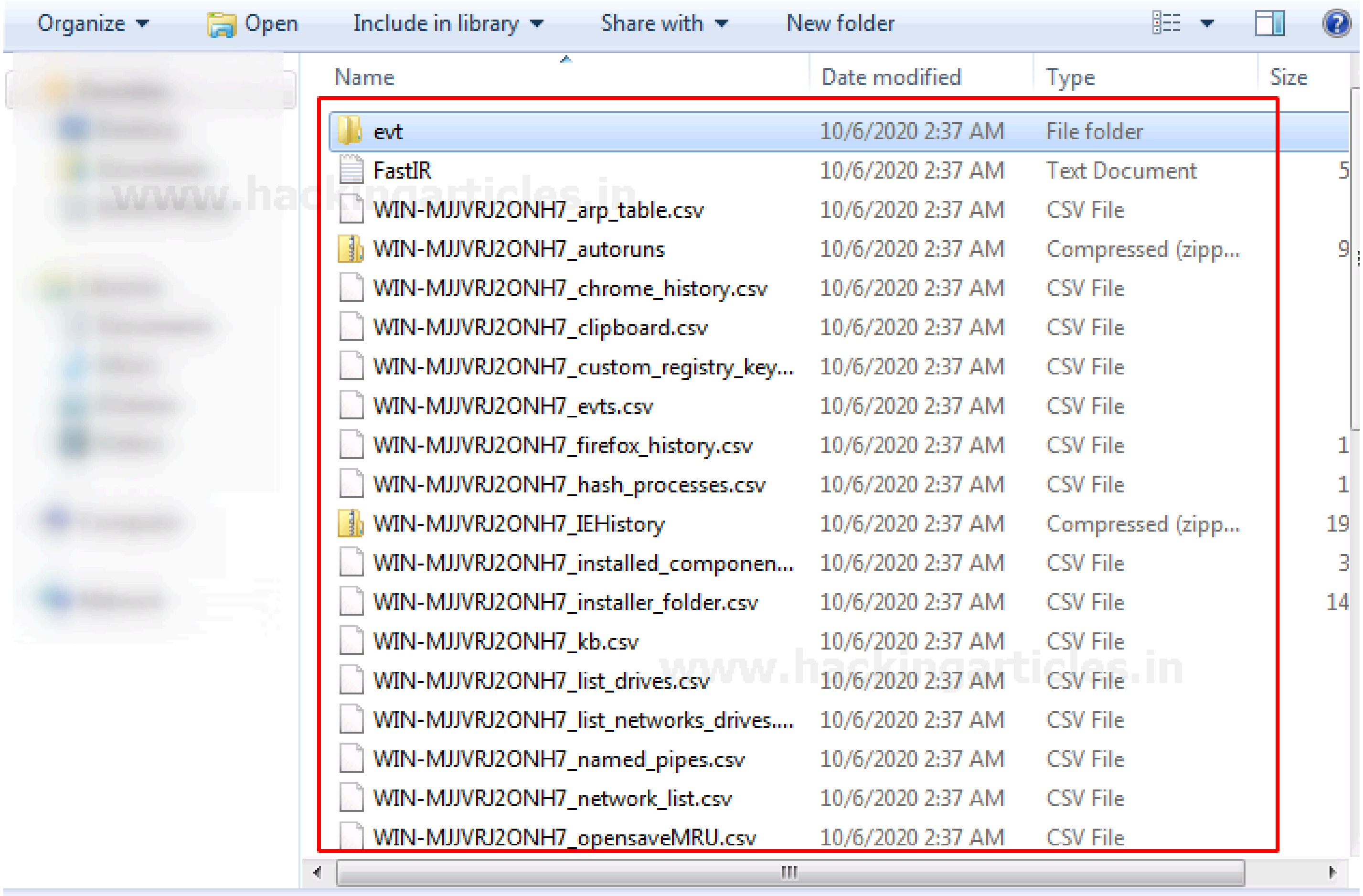
Let’s begin by exploring how the tool works:

You just need to run the executable file of the tool as administrator and it will automatically start the process of collecting data.



```
C:\Users\raj\Desktop\FastIR_x64.exe

    A forensic analysis tool
```

Results are stored in the folder by the named **output** within the same folder where the executable file is stored.



Name	Date modified	Type	Size
evt	10/6/2020 2:37 AM	File folder	
FastIR	10/6/2020 2:37 AM	Text Document	5
WIN-MJJVRJ2ONH7_arp_table.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_autoruns	10/6/2020 2:37 AM	Compressed (zipp...	9
WIN-MJJVRJ2ONH7_chrome_history.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_clipboard.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_custom_registry_key...	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_evts.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_firefox_history.csv	10/6/2020 2:37 AM	CSV File	1
WIN-MJJVRJ2ONH7_hash_processes.csv	10/6/2020 2:37 AM	CSV File	1
WIN-MJJVRJ2ONH7_IEHistory	10/6/2020 2:37 AM	Compressed (zipp...	19
WIN-MJJVRJ2ONH7_installed_componen...	10/6/2020 2:37 AM	CSV File	3
WIN-MJJVRJ2ONH7_installer_folder.csv	10/6/2020 2:37 AM	CSV File	14
WIN-MJJVRJ2ONH7_kb.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_list_drives.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_list_networks_drives....	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_named_pipes.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_network_list.csv	10/6/2020 2:37 AM	CSV File	
WIN-MJJVRJ2ONH7_opensaveMRU.csv	10/6/2020 2:37 AM	CSV File	

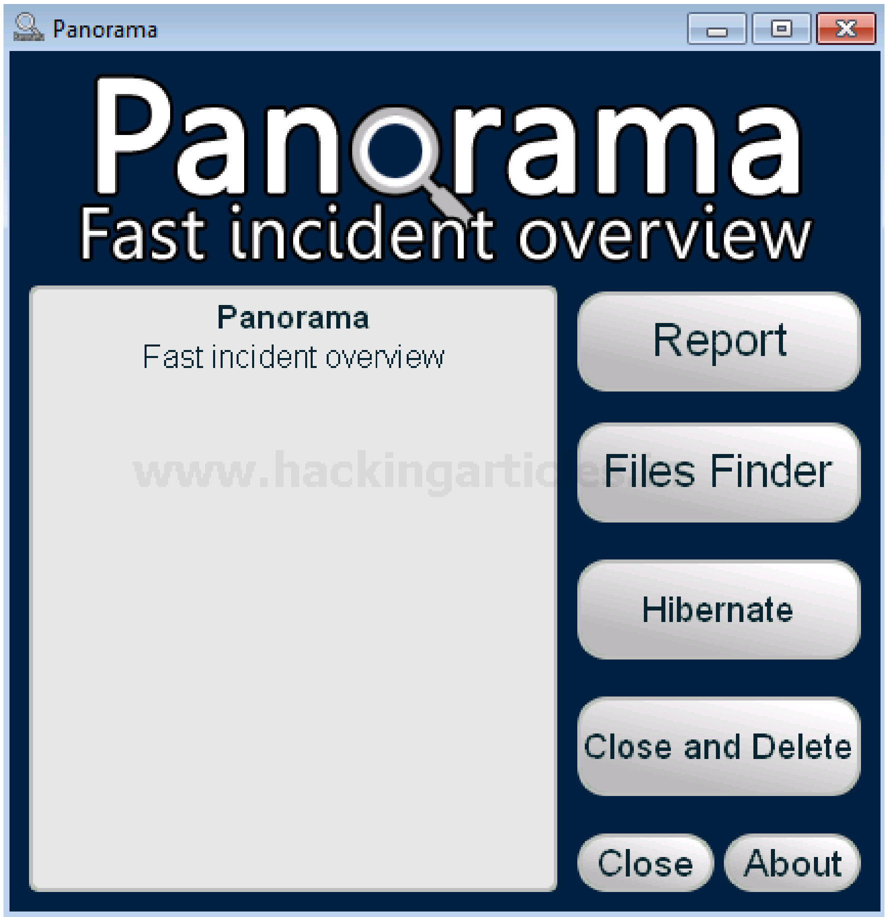
Panorama

Panorama is a tool that creates a fast report of the incident on the Windows system.

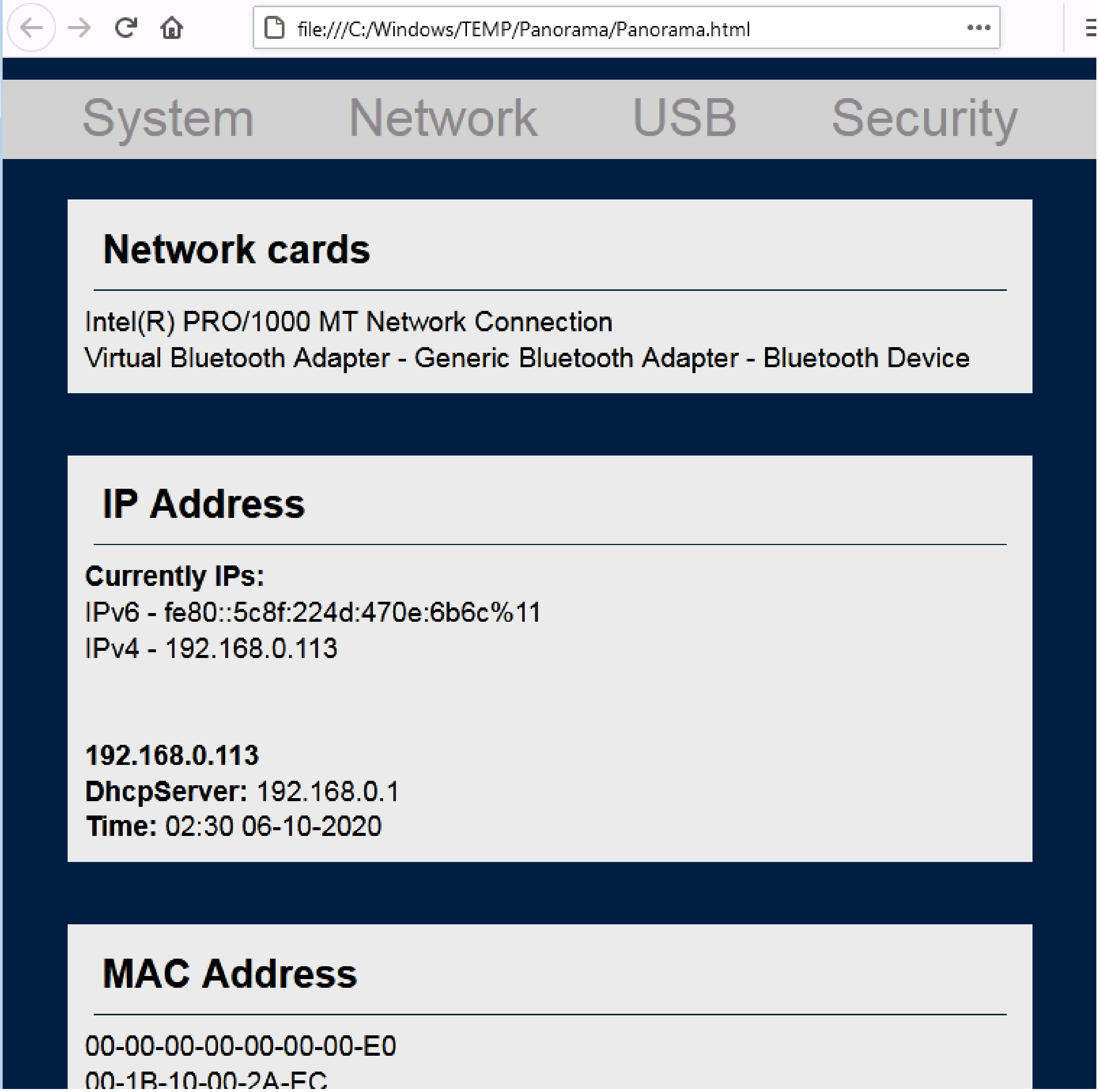
You can download the tool from **here**.

Let’s begin by exploring how the tool works:

- Run the Panorama.exe on the system.
- Choose “Report” to create a fast incident overview.



The browser will automatically launch the report after the process is completed.



Network cards

Intel(R) PRO/1000 MT Network Connection
Virtual Bluetooth Adapter - Generic Bluetooth Adapter - Bluetooth Device

IP Address

Currently IPs:
IPv6 - fe80::5c8f:224d:470e:6b6c%11
IPv4 - 192.168.0.113

192.168.0.113
DhcpServer: 192.168.0.1
Time: 02:30 06-10-2020

MAC Address

00-00-00-00-00-00-00-E0
00-1B-10-00-2A-EC

The report data is distributed in a different section as a system, network, USB, security, and others.

Triage

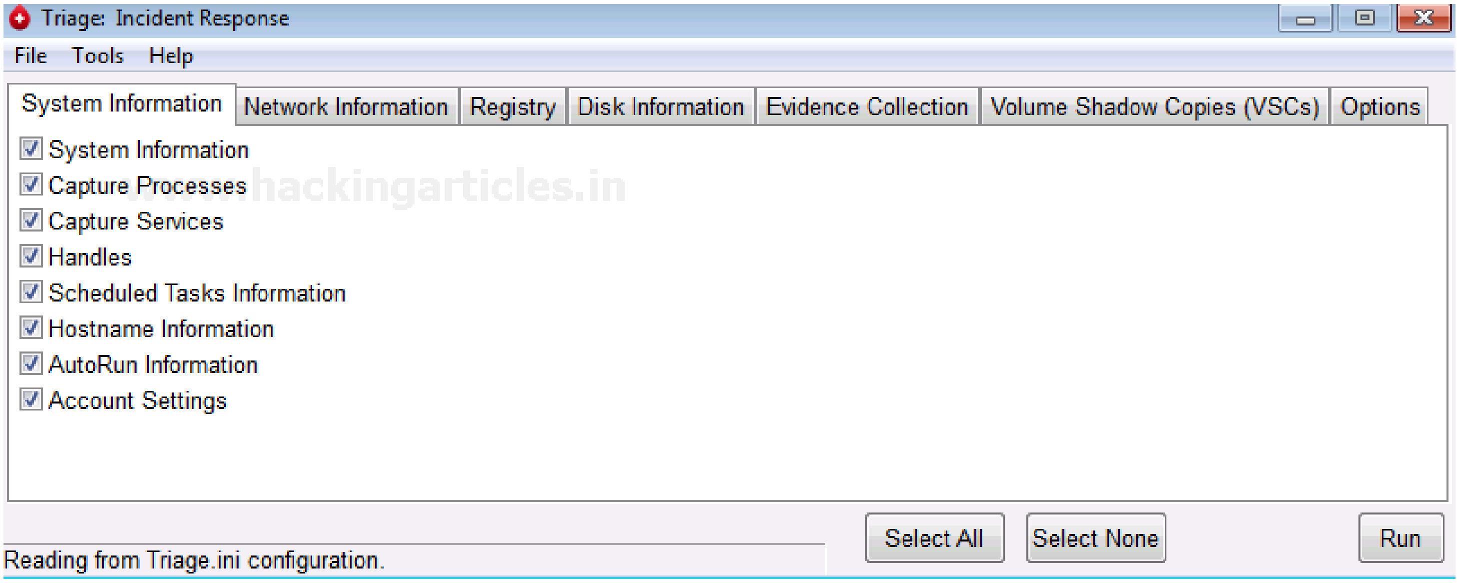
Triage is an incident response tool that automatically collects information for the Windows operating system. Triage-ir is a script written by Michael Ahrendt.

You can simply select the data you want to collect using the checkboxes given right under each tab. Triage IR requires the Sysinternals toolkit for successful execution.

Download **here**.

Let’s begin by exploring how the tool works:

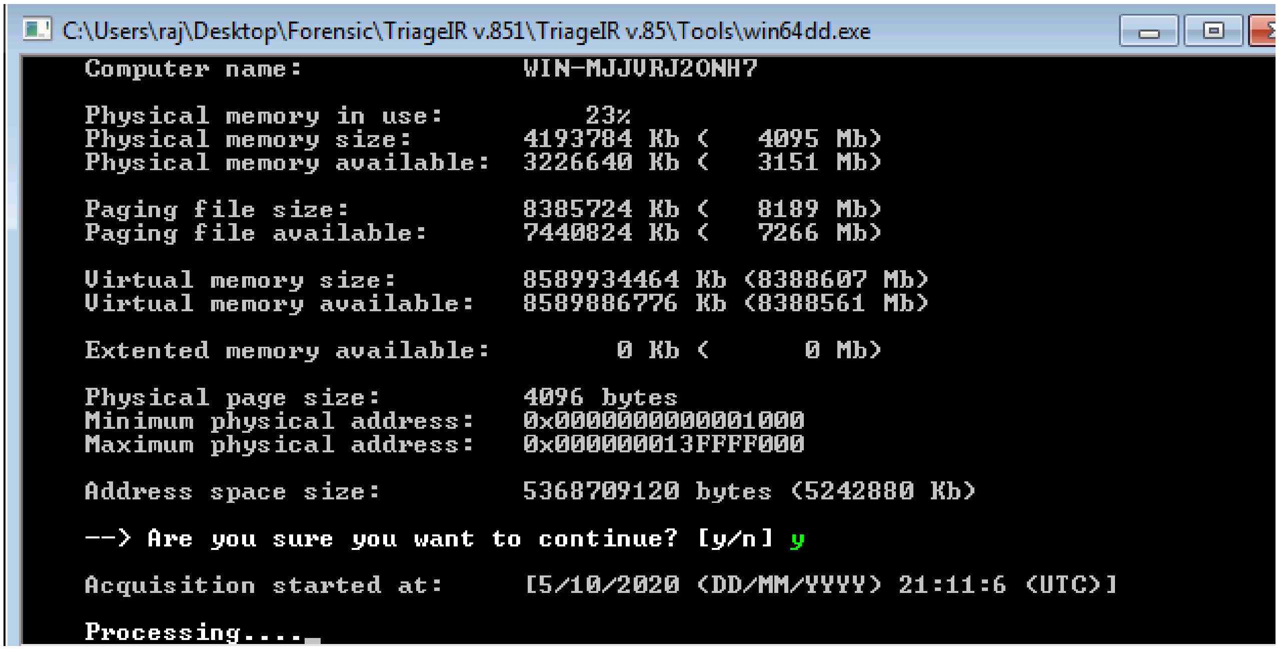
- Run the executable file of the tool.
- Select “Yes” when shows the prompt to introduce the Sysinternal toolkit.



☑ System Information
☑ Capture Processes
☑ Capture Services
☑ Handles
☑ Scheduled Tasks Information
☑ Hostname Information
☑ AutoRun Information
☑ Account Settings

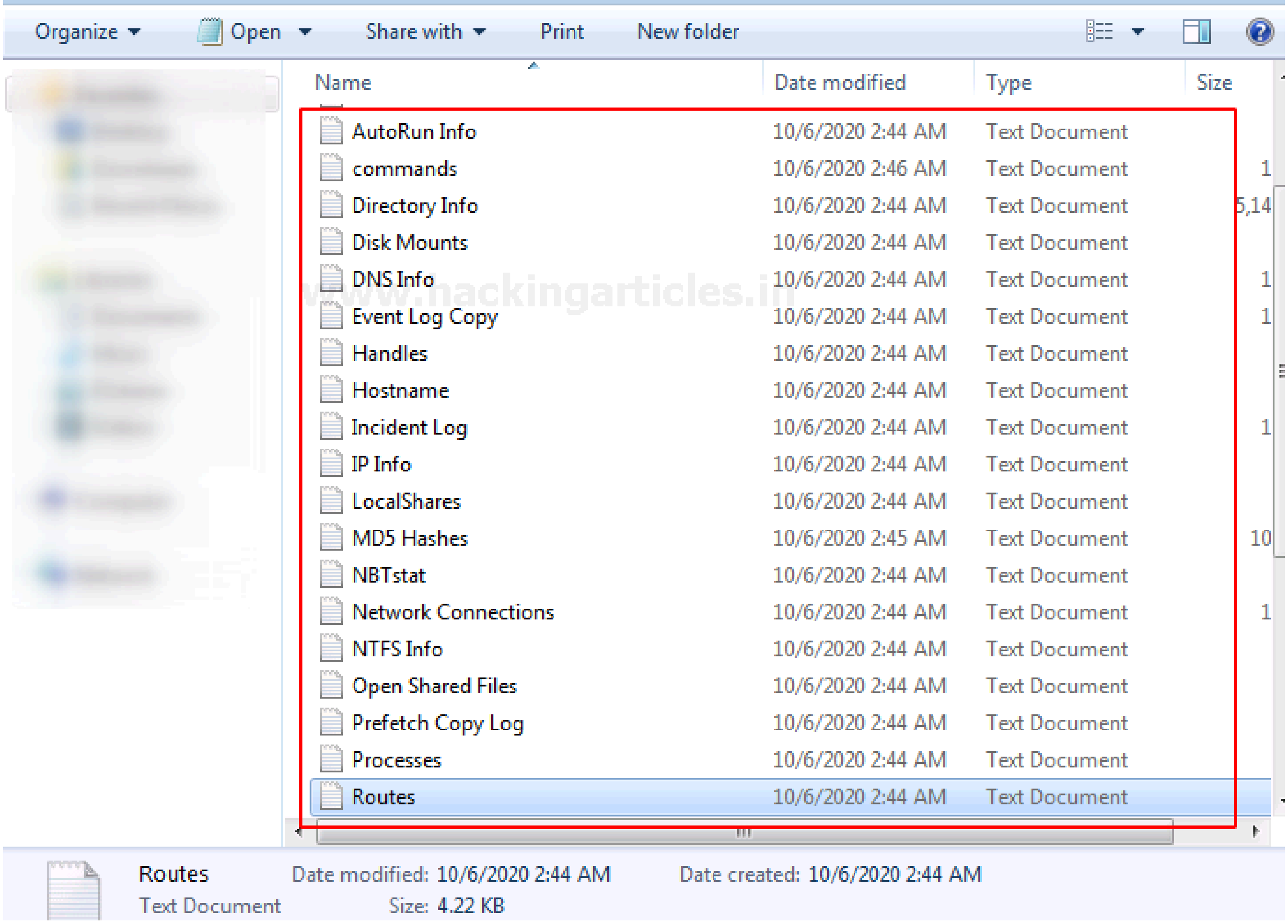
Reading from Triage.ini configuration.

Click on “Run” after picking the data to gather. The process of data collection will take a couple of minutes to complete.


C:\Users\raj\Desktop\Forensic\TriageIR v.851\TriageIR v.85\Tools\win64dd.exe

```
Computer name:               WIN-MJJVRJ2ONH7

Physical memory in use:          23%
Physical memory size:        4193784 Kb (   4095 Mb)
Physical memory available:   3226640 Kb (   3151 Mb)

Paging file size:            8385724 Kb (   8189 Mb)
Paging file available:       7440824 Kb (   7266 Mb)

Virtual memory size:         8589934464 Kb (8388607 Mb)
Virtual memory available:    8589886776 Kb (8388561 Mb)

Extented memory available:         0 Kb (      0 Mb)

Physical page size:          4096 bytes
Minimum physical address:    0x0000000000001000
Maximum physical address:    0x000000013FFFF000

Address space size:          5368709120 bytes (5242880 Kb)

--> Are you sure you want to continue? [y/n] y

Acquisition started at:      [5/10/2020 (DD/MM/YYYY) 21:11:6 (UTC)]

Processing....
```

The data is collected in the folder by the name of your computer alongside the date at the same destination as the executable file of the tool.



Name	Date modified	Type	Size
AutoRun Info	10/6/2020 2:44 AM	Text Document	
commands	10/6/2020 2:46 AM	Text Document	1
Directory Info	10/6/2020 2:44 AM	Text Document	5,14
Disk Mounts	10/6/2020 2:44 AM	Text Document	
DNS Info	10/6/2020 2:44 AM	Text Document	1
Event Log Copy	10/6/2020 2:44 AM	Text Document	1
Handles	10/6/2020 2:44 AM	Text Document	
Hostname	10/6/2020 2:44 AM	Text Document	
Incident Log	10/6/2020 2:44 AM	Text Document	1
IP Info	10/6/2020 2:44 AM	Text Document	
LocalShares	10/6/2020 2:44 AM	Text Document	
MD5 Hashes	10/6/2020 2:45 AM	Text Document	10
NBTstat	10/6/2020 2:44 AM	Text Document	
Network Connections	10/6/2020 2:44 AM	Text Document	1
NTFS Info	10/6/2020 2:44 AM	Text Document	
Open Shared Files	10/6/2020 2:44 AM	Text Document	
Prefetch Copy Log	10/6/2020 2:44 AM	Text Document	
Processes	10/6/2020 2:44 AM	Text Document	
Routes	10/6/2020 2:44 AM	Text Document	

Routes Date modified: 10/6/2020 2:44 AM Date created: 10/6/2020 2:44 AM
Text Document Size: 4.22 KB

IREC – IR Evidence Collector | Binalyze

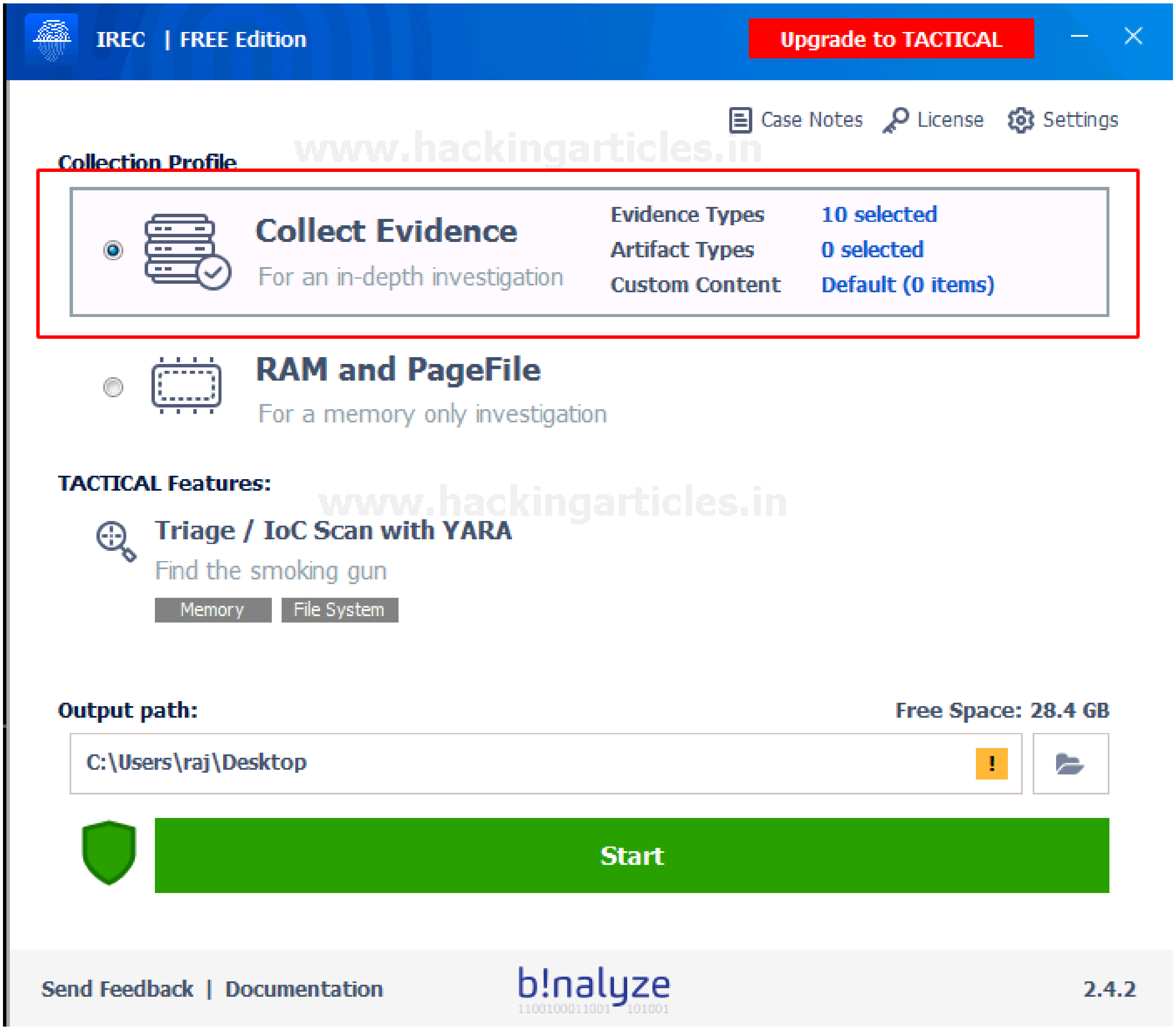
IREC is a forensic evidence collection tool that is easy to use the tool. It is an all-in-one tool, user-friendly as well as malware resistant. This tool is created by **Binalyze**. A paid version of this tool is also available.
Download the tool from **here**.

Let's begin by exploring how the tool works:

You can collect data by two means:

- Collect evidence: This is for an in-depth investigation.
- RAM and Page file: This is for memory only investigation

Here we will choose, "collect evidence." for in-depth evidence. Click start to proceed further.



Collection Profile

● Collect Evidence
For an in-depth investigation

Evidence Types	10 selected
Artifact Types	0 selected
Custom Content	Default (0 items)

○ RAM and PageFile
For a memory only investigation

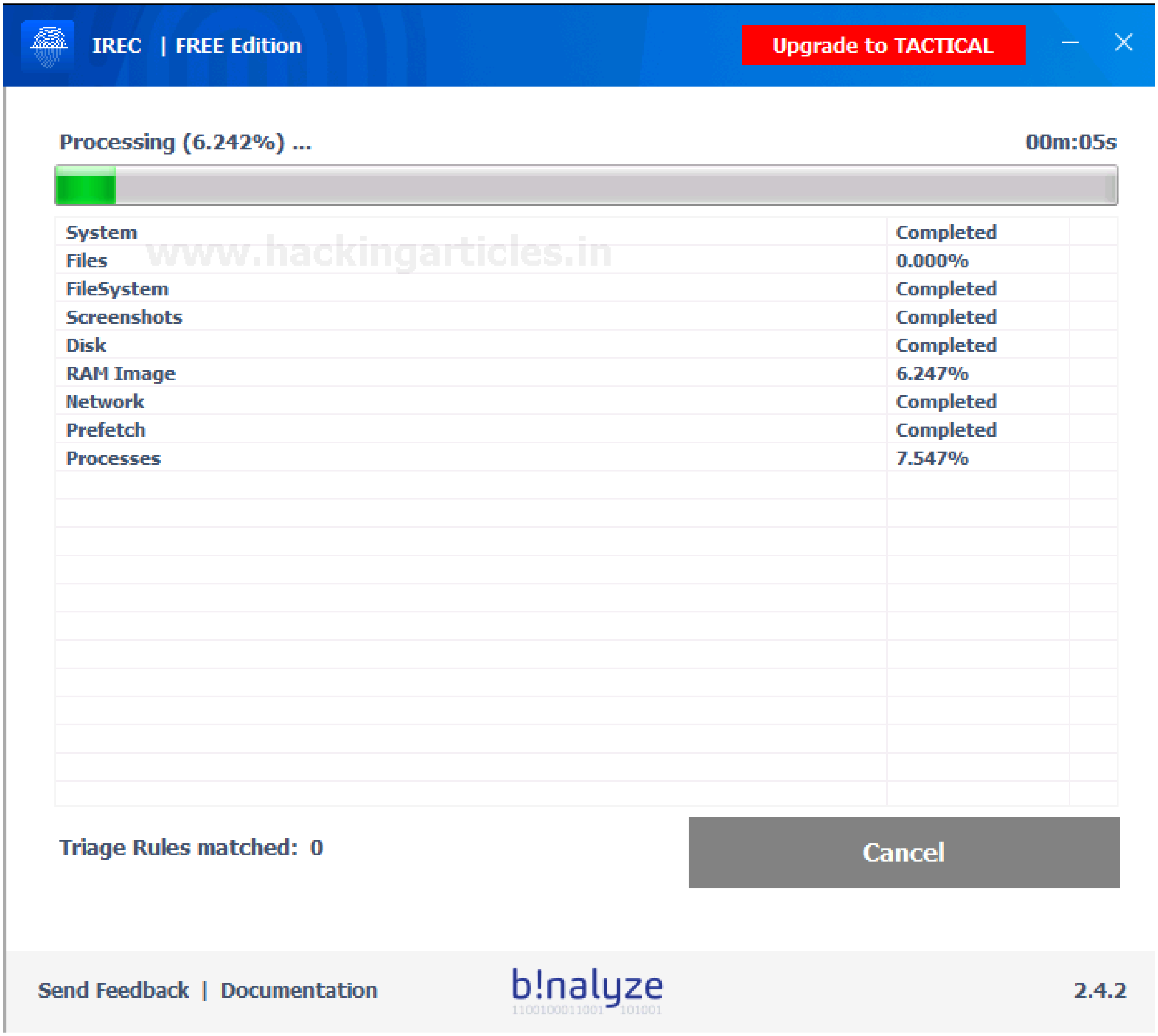
TACTICAL Features:

Triage / IoC Scan with YARA
Find the smoking gun

Output path: Free Space: 28.4 GB

C:\Users\raj\Desktop

The process has been begun after effectively picking the collection profile.

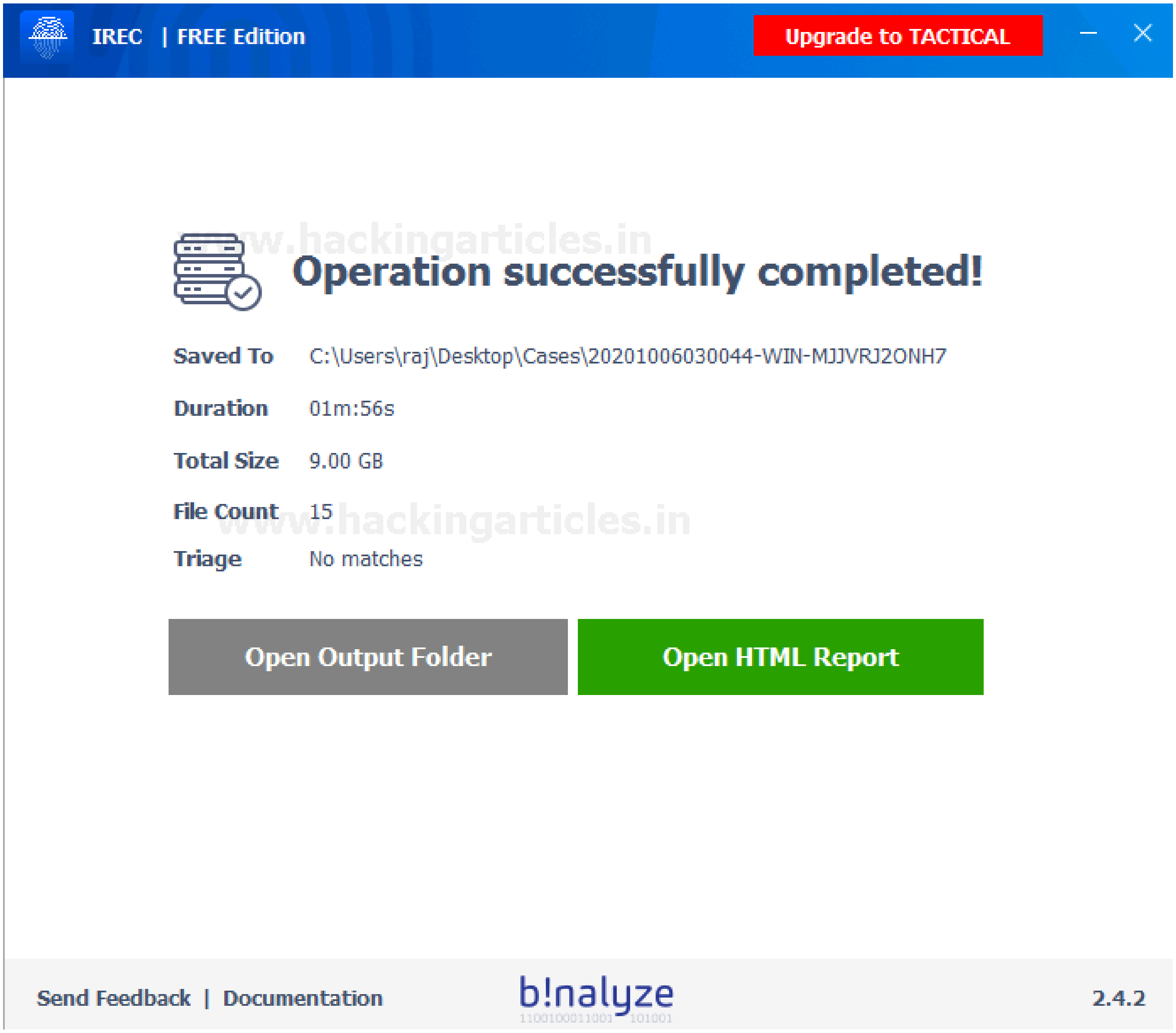


Processing (6.242%) ... 00m:05s

System	Completed
Files	0.000%
FileSystem	Completed
Screenshots	Completed
Disk	Completed
RAM Image	6.247%
Network	Completed
Prefetch	Completed
Processes	7.547%

Triage Rules matched: 0

The process is completed. You can analyze the data collected from the output folder.



Operation successfully completed!

Saved To C:\Users\raj\Desktop\Cases\20201006030044-WIN-MJJVRJ2ONH7

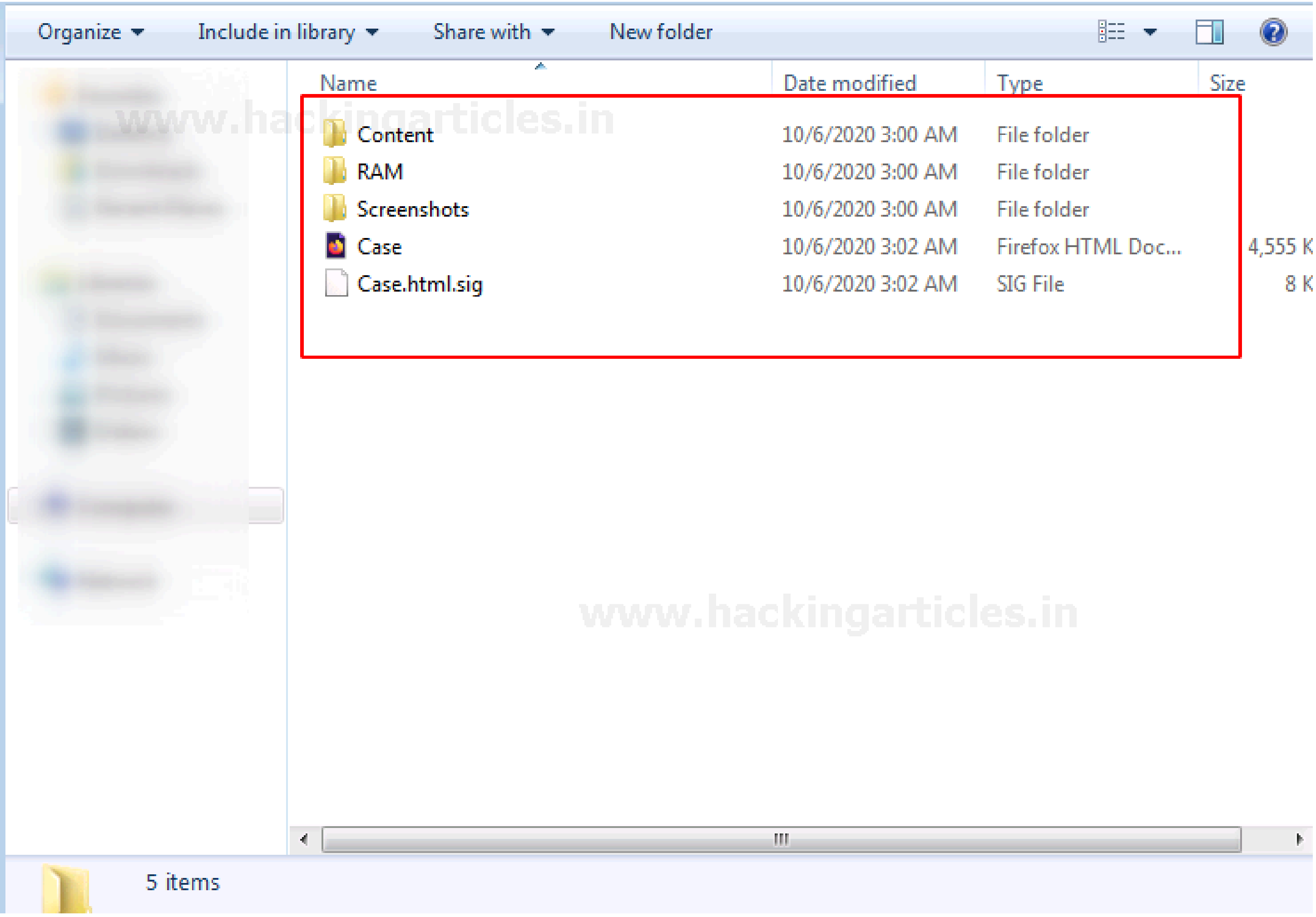
Duration 01m:56s

Total Size 9.00 GB

File Count 15

Triage No matches

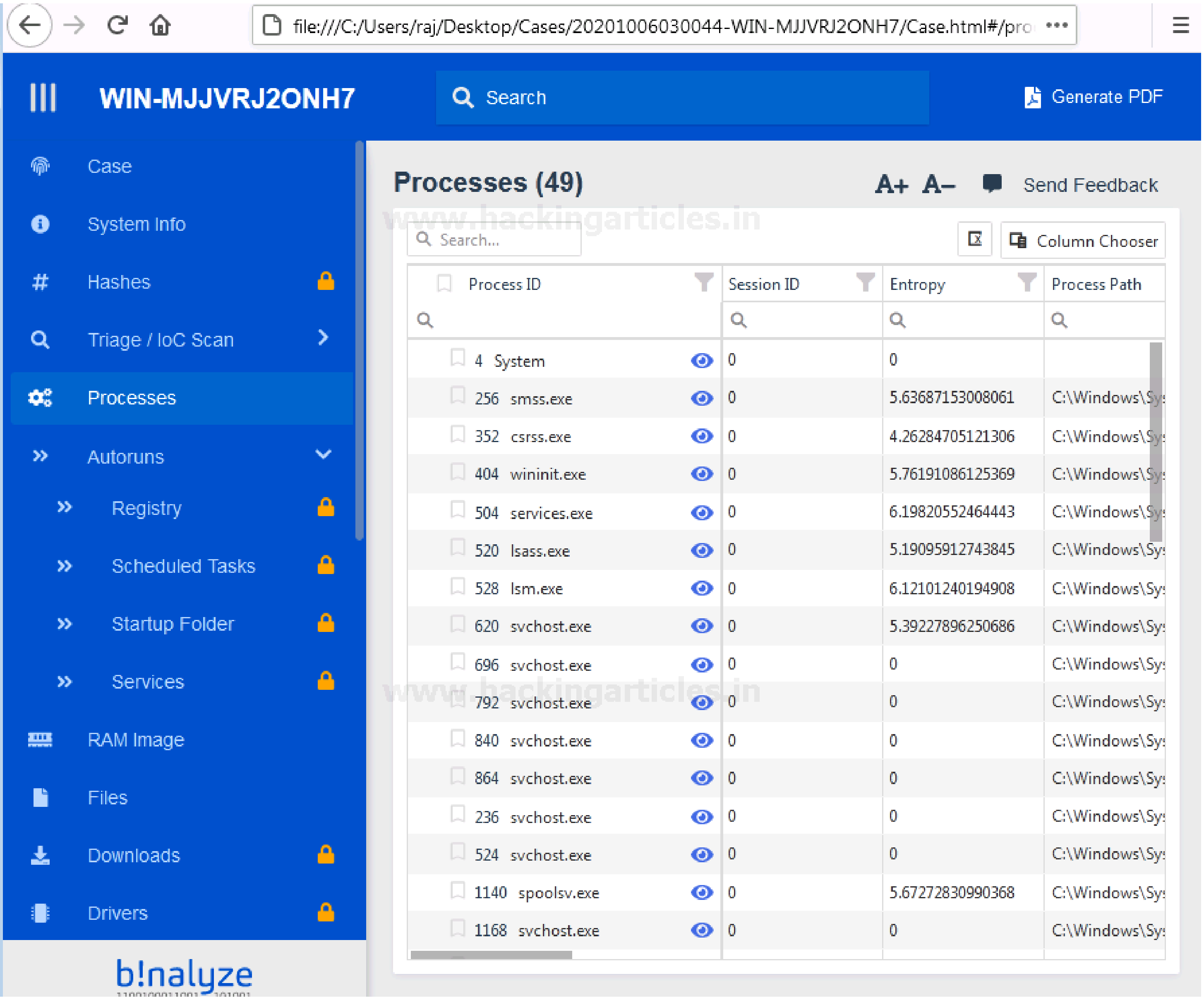
The output will be stored in a folder named **cases** that will comprise of a folder named by PC name and date at the same destination as the executable file of the tool.



Name	Date modified	Type	Size
Content	10/6/2020 3:00 AM	File folder	
RAM	10/6/2020 3:00 AM	File folder	
Screenshots	10/6/2020 3:00 AM	File folder	
Case	10/6/2020 3:02 AM	Firefox HTML Doc...	4,555 K
Case.html.sig	10/6/2020 3:02 AM	SIG File	8 K

5 items

Here is the HTML report of the evidence collection. The HTML report is easy to analyze, the data collected is classified into various sections of evidence. You can also generate the PDF of your report.



Processes (49)

Process ID	Session ID	Entropy	Process Path
4 System	0	0	
256 smss.exe	0	5.63687153008061	C:\Windows\Sy
352 csrss.exe	0	4.26284705121306	C:\Windows\Sy
404 wininit.exe	0	5.76191086125369	C:\Windows\Sy
504 services.exe	0	6.19820552464443	C:\Windows\Sy
520 lsass.exe	0	5.19095912743845	C:\Windows\Sy
528 lsm.exe	0	6.12101240194908	C:\Windows\Sy
620 svchost.exe	0	5.39227896250686	C:\Windows\Sy
696 svchost.exe	0	0	C:\Windows\Sy
792 svchost.exe	0	0	C:\Windows\Sy
840 svchost.exe	0	0	C:\Windows\Sy
864 svchost.exe	0	0	C:\Windows\Sy
236 svchost.exe	0	0	C:\Windows\Sy
524 svchost.exe	0	0	C:\Windows\Sy
1140 spoolsv.exe	0	5.67272830990368	C:\Windows\Sy
1168 svchost.exe	0	0	C:\Windows\Sy

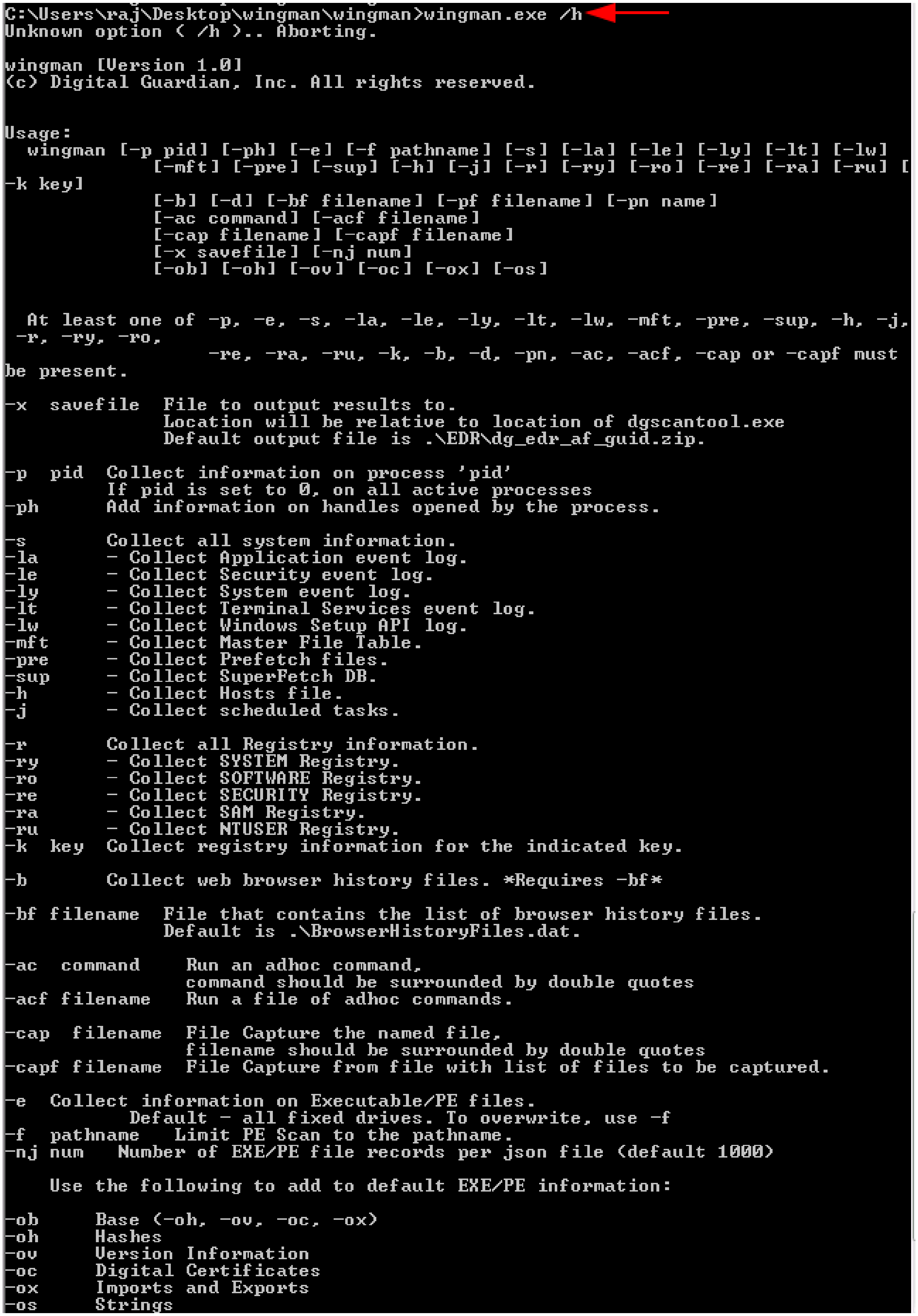
DG Wingman

DG Wingman is a free windows tool for forensic artifacts collection and analysis. The tool is by **DigitalGuardian**. This tool collects artifacts of importance such as registry logs, system logs, browser history, and many more. Also allows you to execute commands as per the need for data collection.

You can download the tool from **here**.

Let's begin by exploring how the tool works:

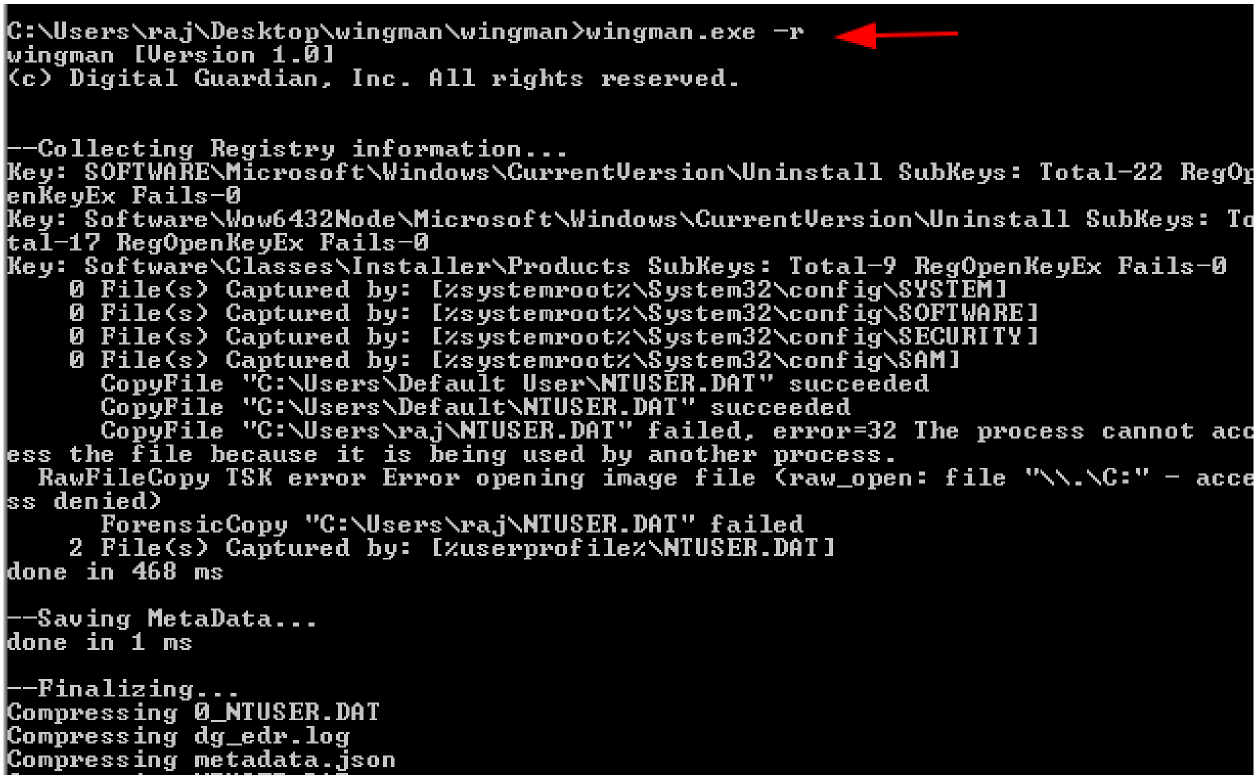
- Run the executable file of the tool.
- Use the command wingman.exe/**h,** this gives you a rundown of commands along with their capacities.



```
C:\Users\raj\Desktop\wingman\wingman>wingman.exe /h
Unknown option ( /h ).. Aborting.

wingman [Version 1.0]
(c) Digital Guardian, Inc. All rights reserved.


Usage:
  wingman [-p pid] [-ph] [-e] [-f pathname] [-s] [-la] [-le] [-ly] [-lt] [-lw]
             [-mft] [-pre] [-sup] [-h] [-j] [-r] [-ry] [-ro] [-re] [-ra] [-ru] [
-k key]
             [-b] [-d] [-bf filename] [-pf filename] [-pn name]
             [-ac command] [-acf filename]
             [-cap filename] [-capf filename]
             [-x savefile] [-nj num]
             [-ob] [-oh] [-ov] [-oc] [-ox] [-os]


  At least one of -p, -e, -s, -la, -le, -ly, -lt, -lw, -mft, -pre, -sup, -h, -j,
 -r, -ry, -ro,
                  -re, -ra, -ru, -k, -b, -d, -pn, -ac, -acf, -cap or -capf must
be present.

-x  savefile  File to output results to.
              Location will be relative to location of dgscantool.exe
              Default output file is .\EDR\dg_edr_af_guid.zip.

-p  pid  Collect information on process 'pid'
         If pid is set to 0, on all active processes
-ph      Add information on handles opened by the process.

-s       Collect all system information.
-la      - Collect Application event log.
-le      - Collect Security event log.
-ly      - Collect System event log.
-lt      - Collect Terminal Services event log.
-lw      - Collect Windows Setup API log.
-mft     - Collect Master File Table.
-pre     - Collect Prefetch files.
-sup     - Collect SuperFetch DB.
-h       - Collect Hosts file.
-j       - Collect scheduled tasks.

-r       Collect all Registry information.
-ry      - Collect SYSTEM Registry.
-ro      - Collect SOFTWARE Registry.
-re      - Collect SECURITY Registry.
-ra      - Collect SAM Registry.
-ru      - Collect NTUSER Registry.
-k  key  Collect registry information for the indicated key.

-b       Collect web browser history files. *Requires -bf*

-bf filename  File that contains the list of browser history files.
              Default is .\BrowserHistoryFiles.dat.

-ac  command    Run an adhoc command,
                command should be surrounded by double quotes
-acf filename   Run a file of adhoc commands.

-cap  filename  File Capture the named file,
                filename should be surrounded by double quotes
-capf filename  File Capture from file with list of files to be captured.

-e  Collect information on Executable/PE files.
           Default - all fixed drives. To overwrite, use -f
-f  pathname   Limit PE Scan to the pathname.
-nj num   Number of EXE/PE file records per json file (default 1000)

    Use the following to add to default EXE/PE information:

-ob     Base (-oh, -ov, -oc, -ox)
-oh     Hashes
-ov     Version Information
-oc     Digital Certificates
-ox     Imports and Exports
-os     Strings
```

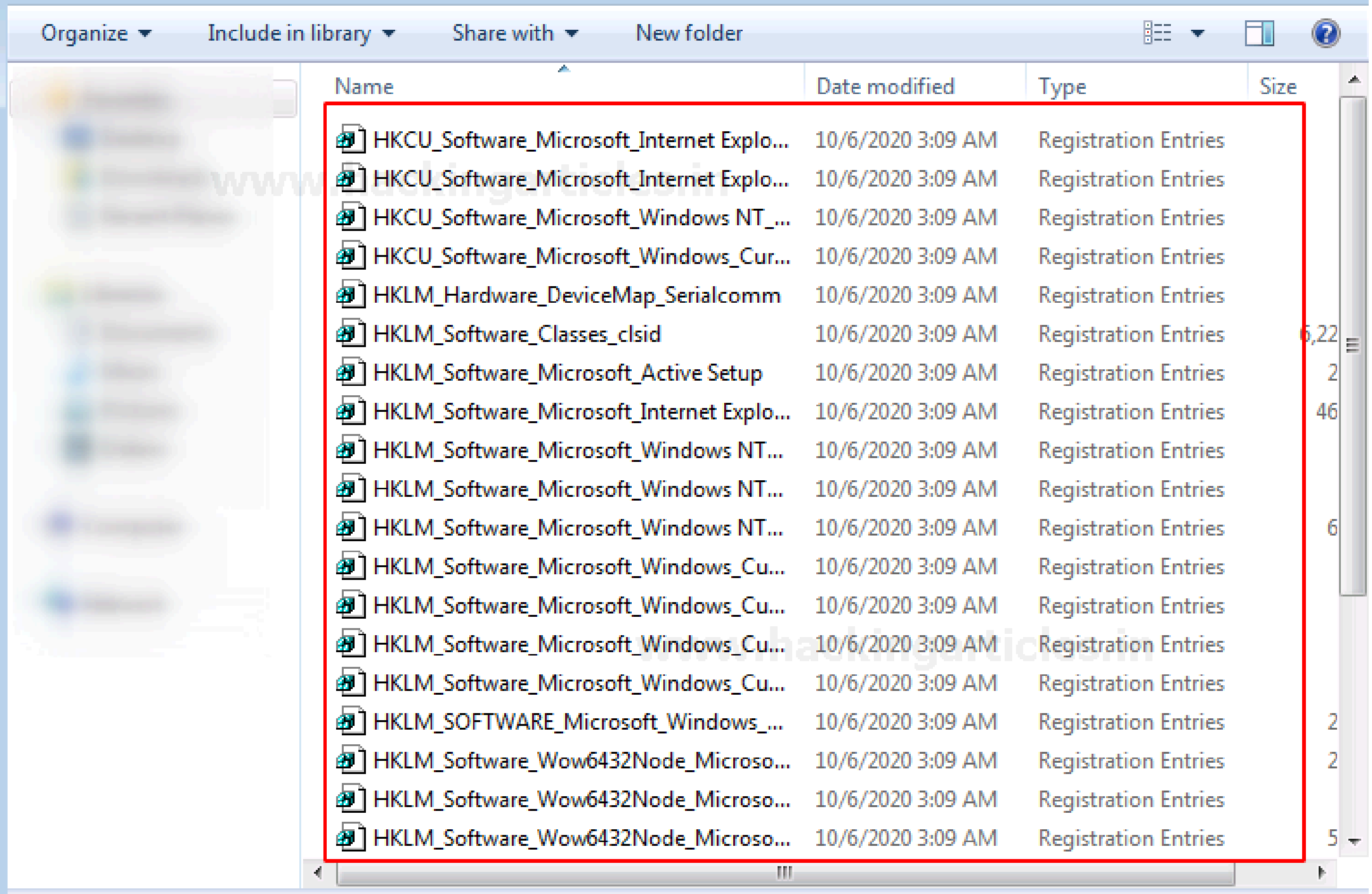
For example, in the incident, we need to gather the registry logs. We will use the command

```
wingman.exe -r
```



```
C:\Users\raj\Desktop\wingman\wingman>wingman.exe -r
wingman [Version 1.0]
(c) Digital Guardian, Inc. All rights reserved.


--Collecting Registry information...
Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall SubKeys: Total-22 RegOp
enKeyEx Fails-0
Key: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall SubKeys: To
tal-17 RegOpenKeyEx Fails-0
Key: Software\Classes\Installer\Products SubKeys: Total-9 RegOpenKeyEx Fails-0
    0 File(s) Captured by: [%systemroot%\System32\config\SYSTEM]
    0 File(s) Captured by: [%systemroot%\System32\config\SOFTWARE]
    0 File(s) Captured by: [%systemroot%\System32\config\SECURITY]
    0 File(s) Captured by: [%systemroot%\System32\config\SAM]
      CopyFile "C:\Users\Default User\NTUSER.DAT" succeeded
      CopyFile "C:\Users\Default\NTUSER.DAT" succeeded
      CopyFile "C:\Users\raj\NTUSER.DAT" failed, error=32 The process cannot acc
ess the file because it is being used by another process.
  RawFileCopy TSK error Error opening image file (raw_open: file "\\.\C:" - acce
ss denied)
      ForensicCopy "C:\Users\raj\NTUSER.DAT" failed
    2 File(s) Captured by: [%userprofile%\NTUSER.DAT]
done in 468 ms

--Saving MetaData...
done in 1 ms

--Finalizing...
Compressing 0_NTUSER.DAT
Compressing dg_edr.log
Compressing metadata.json
```

All the registry entries are collected successfully.



Name	Date modified	Type	Size
HKCU_Software_Microsoft_Internet Explo...	10/6/2020 3:09 AM	Registration Entries	
HKCU_Software_Microsoft_Internet Explo...	10/6/2020 3:09 AM	Registration Entries	
HKCU_Software_Microsoft_Windows NT_...	10/6/2020 3:09 AM	Registration Entries	
HKCU_Software_Microsoft_Windows_Cur...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Hardware_DeviceMap_Serialcomm	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Classes_clsid	10/6/2020 3:09 AM	Registration Entries	6,22
HKLM_Software_Microsoft_Active Setup	10/6/2020 3:09 AM	Registration Entries	2
HKLM_Software_Microsoft_Internet Explo...	10/6/2020 3:09 AM	Registration Entries	46
HKLM_Software_Microsoft_Windows NT...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Microsoft_Windows NT...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Microsoft_Windows NT...	10/6/2020 3:09 AM	Registration Entries	6
HKLM_Software_Microsoft_Windows_Cu...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Microsoft_Windows_Cu...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Microsoft_Windows_Cu...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Microsoft_Windows_Cu...	10/6/2020 3:09 AM	Registration Entries	
HKLM_SOFTWARE_Microsoft_Windows_...	10/6/2020 3:09 AM	Registration Entries	2
HKLM_Software_Wow6432Node_Microso...	10/6/2020 3:09 AM	Registration Entries	2
HKLM_Software_Wow6432Node_Microso...	10/6/2020 3:09 AM	Registration Entries	
HKLM_Software_Wow6432Node_Microso...	10/6/2020 3:09 AM	Registration Entries	5

These are the amazing tools for first responders. And they even speed up your work as an incident responder. These tools come handy as they facilitate us with both data analyses, fast first responding with additional features.