Forensic Investigation of RAW Image using Forensics Explorer (Part 1)

September 27, 2015 By Raj Chandel

Forensic Explorer is a tool for the analysis of electronic evidence. Primary users of this software are law enforcement, corporate investigations agencies and law firms. Forensic Explorer has the features you expect from the very latest in forensic software. Inclusive with Mount Image Pro, Forensic Explorer will quickly become an important part of your forensic software toolkit.

It enables investigators to:

Manage the analysis of large volumes of information from multiple sources in a case file structure;

- Access and examine all available data, including hidden and system files, deleted files, file and disk slack and unallocated clusters;
- Automate complex investigation tasks;
- Produce detailed reports; and,
- Provide non forensic investigators a platform to easily review evidence.

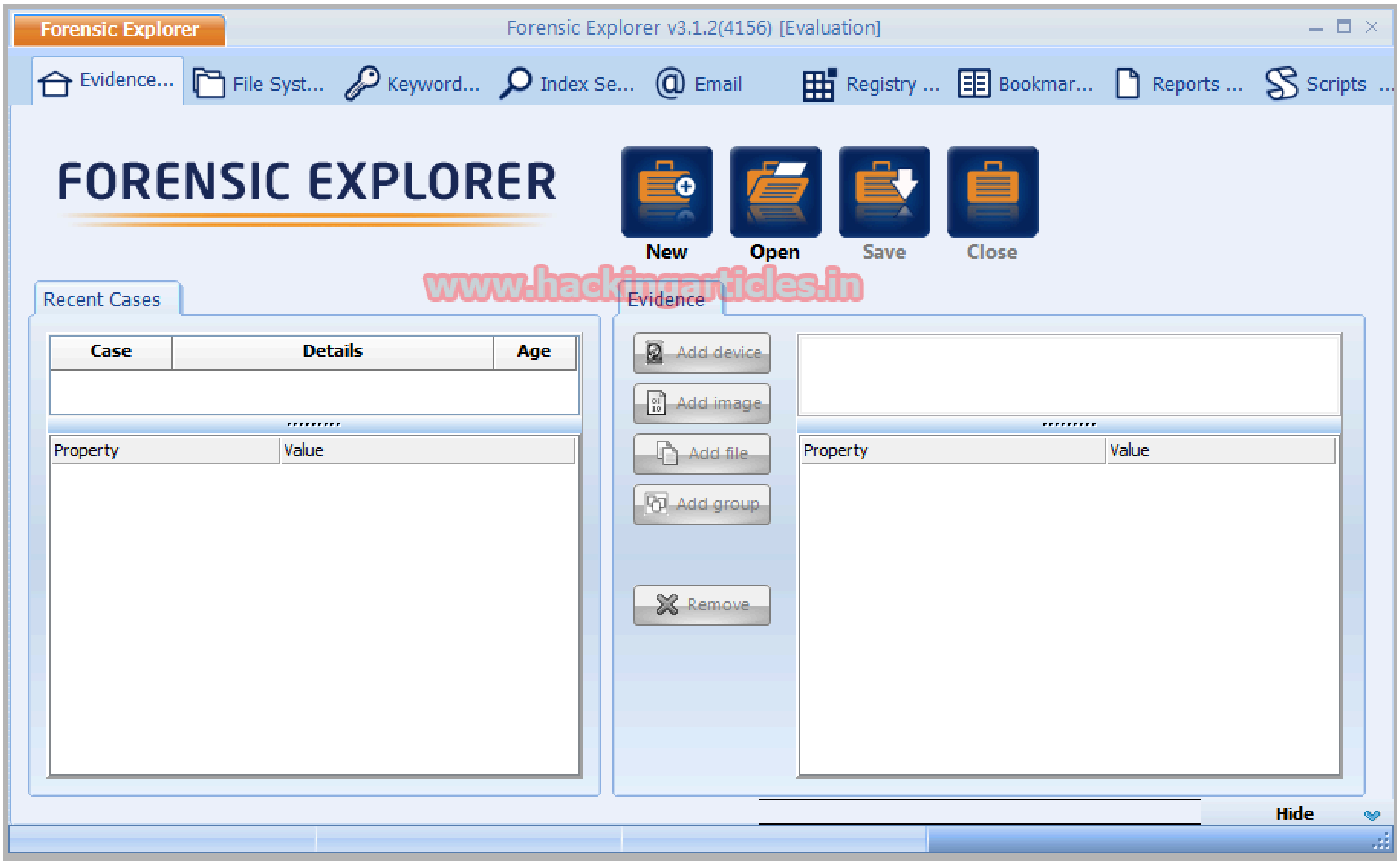
Supported File Formats

Forensics Explorer supports the analysis of the following file formats:

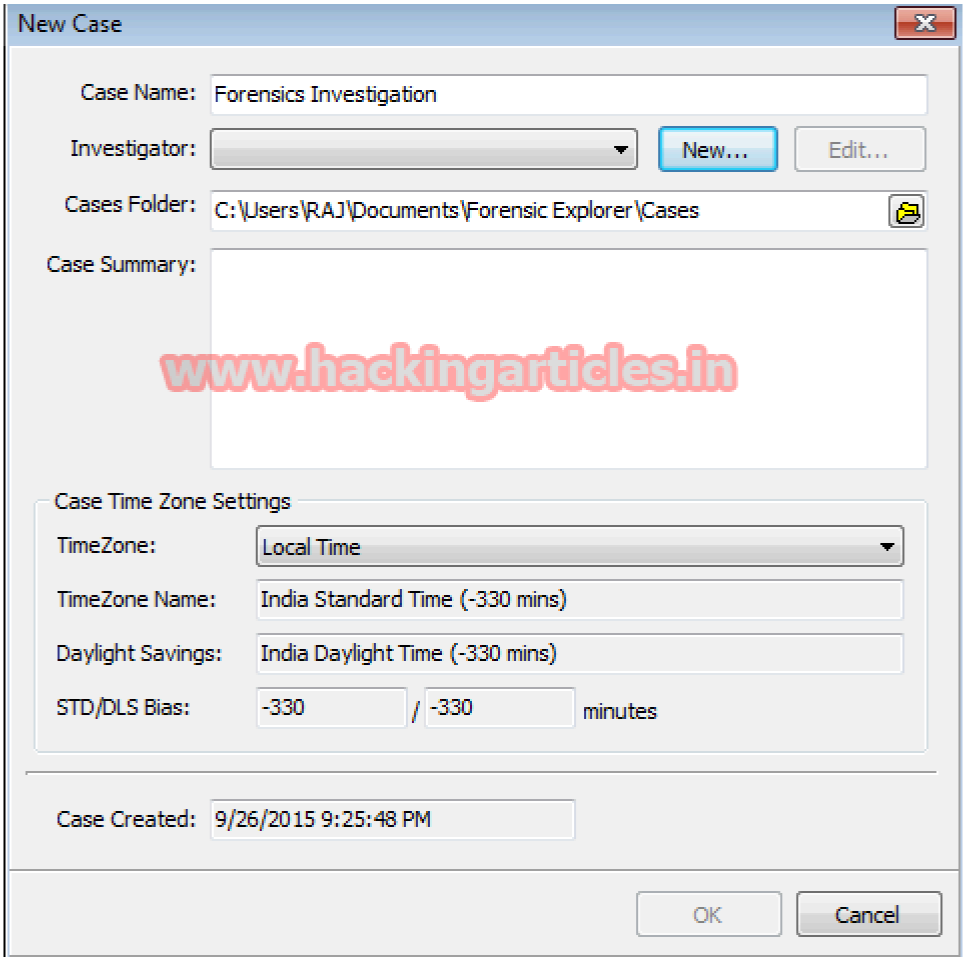
Apple DMG

- DD or RAW;
- EnCase® (.E01, .L01, Ex01);
- Forensic File Format .AFF
- FTK® (.E01, .AD1 formats);
- ISO (CD and DVD image files);
- Microsoft VHD
- NUIX File Safe MFS01
- ProDiscover®
- SMART®
- VMWare®
- XWays E01 and CTR

First Download Forensics Explorer From **here** and install in your pc. And Click on **New** Option.



Enter the **Case Name** and click on **new** option in Investigator TAB


New Case

Case Name: Forensics Investigation

Investigator:

Cases Folder: C:\Users\RAJ\Documents\Forensic Explorer\Cases

Case Summary:

Case Time Zone Settings

TimeZone: Local Time

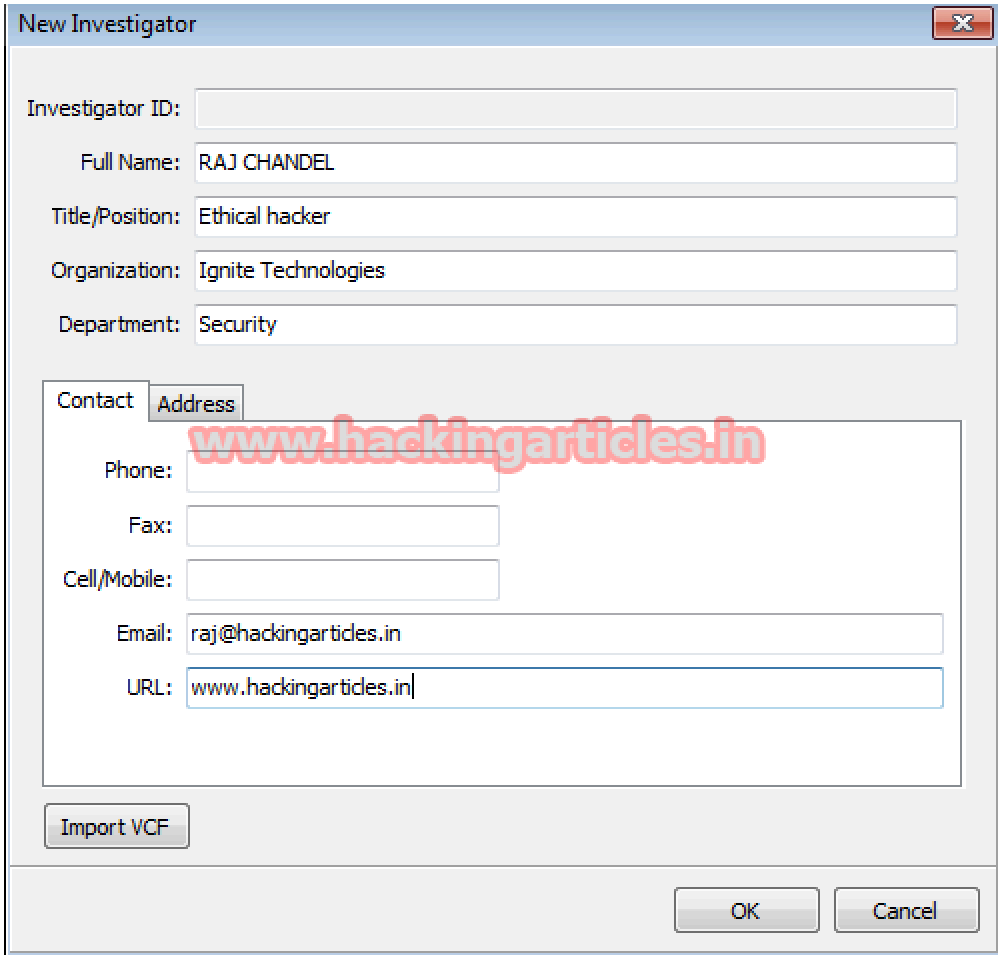
TimeZone Name: India Standard Time (-330 mins)

Daylight Savings: India Daylight Time (-330 mins)

STD/DLS Bias: -330 / -330 minutes

Case Created: 9/26/2015 9:25:48 PM

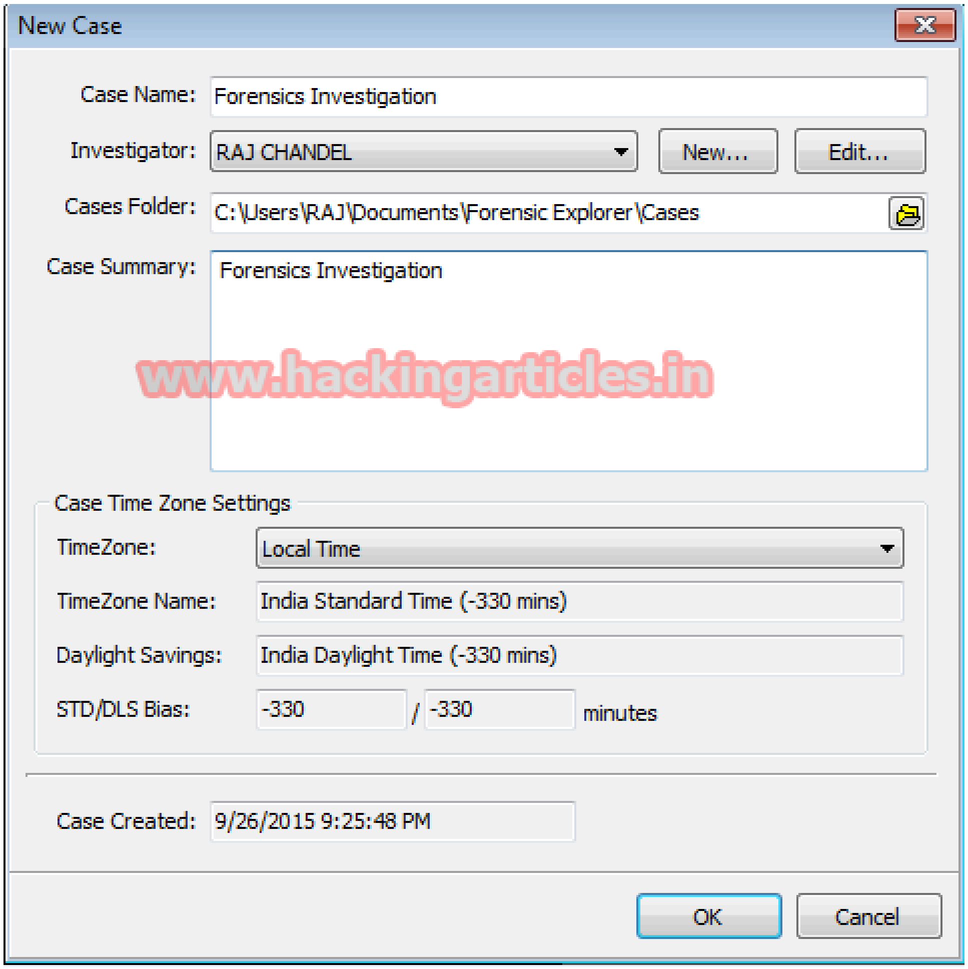
Here in next step you have to enter the **FULL NAME, TITLE,** and **Organization, Department and email details** and click on ok to proceed to next step.



Investigator ID:	
Full Name:	RAJ CHANDEL
Title/Position:	Ethical hacker
Organization:	Ignite Technologies
Department:	Security

Phone:	
Fax:	
Cell/Mobile:	
Email:	raj@hackingarticles.in
URL:	www.hackingarticles.in

Select the **cases folder** where Forensic Evidence will be created. And click on ok



Case Name: Forensics Investigation

Investigator: RAJ CHANDEL

Cases Folder: C:\Users\RAJ\Documents\Forensic Explorer\Cases

Case Summary: Forensics Investigation

Case Time Zone Settings

TimeZone: Local Time

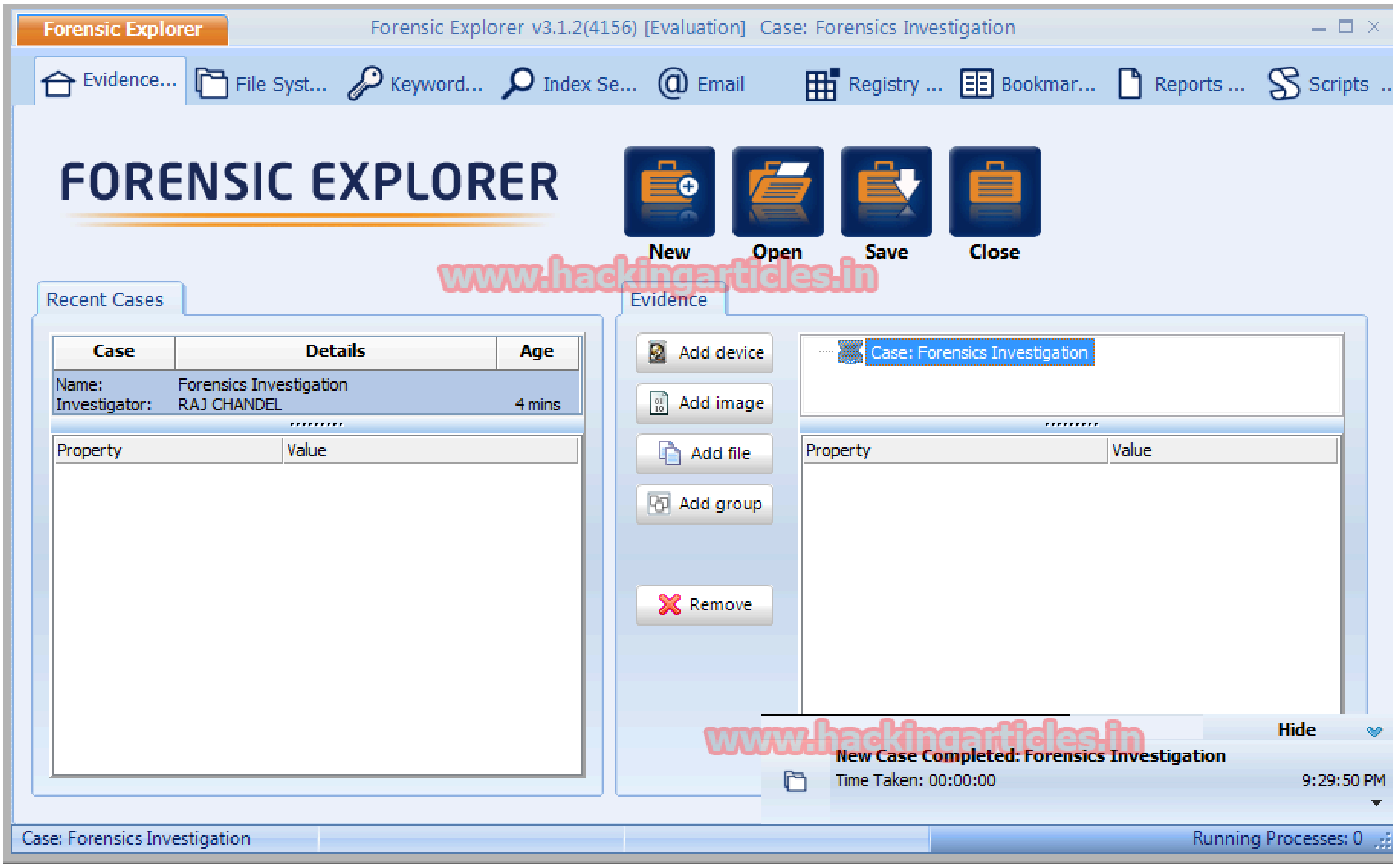
TimeZone Name: India Standard Time (-330 mins)

Daylight Savings: India Daylight Time (-330 mins)

STD/DLS Bias: -330 / -330 minutes

Case Created: 9/26/2015 9:25:48 PM

Now Click '**Add Image.**



Case	Details	Age
Name: Investigator:	Forensics Investigation RAJ CHANDEL	4 mins

Property	Value

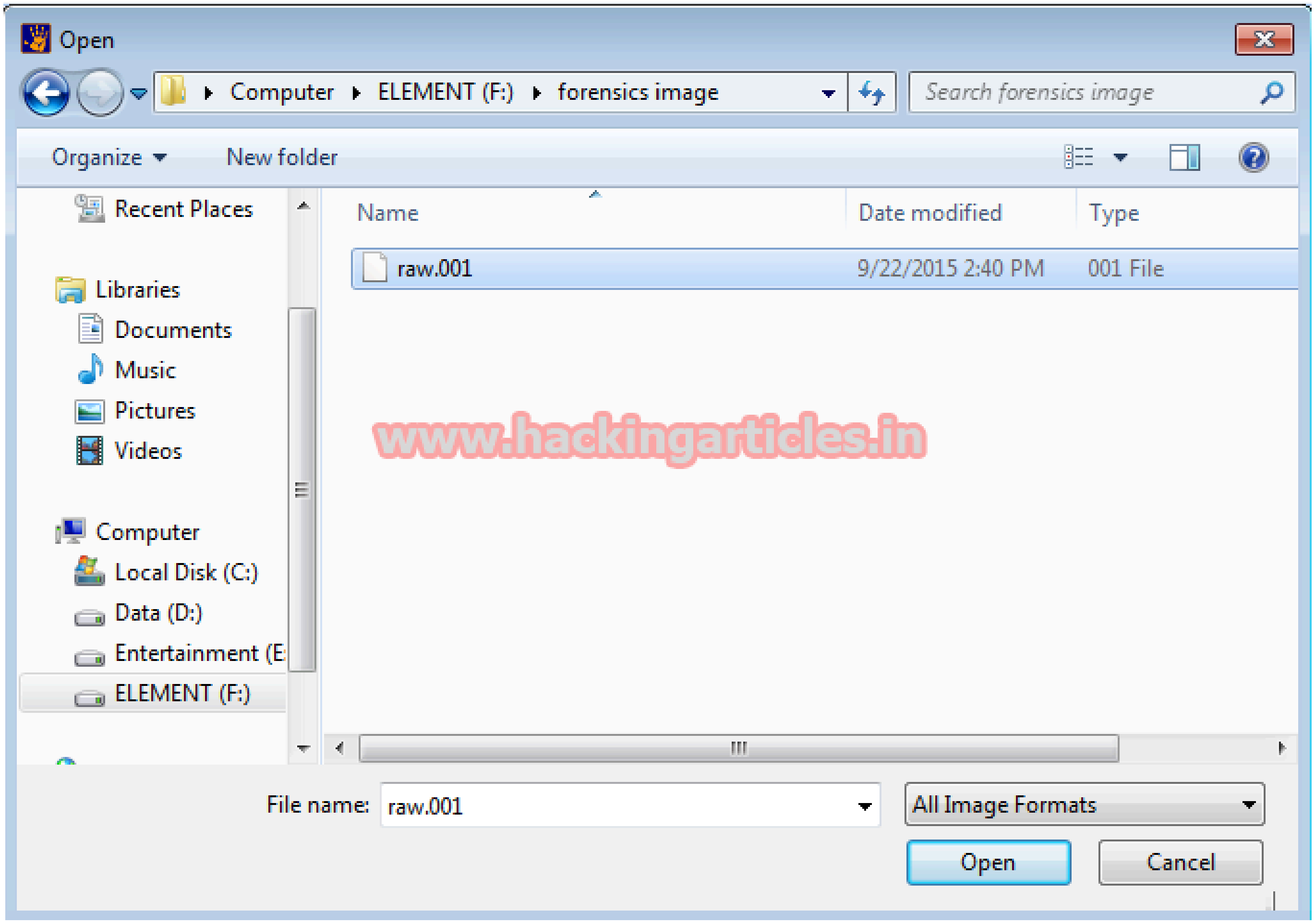
Property	Value

New Case Completed: Forensics Investigation
Time Taken: 00:00:00 9:29:50 PM

Case: Forensics Investigation Running Processes: 0

Now select the path of RAW Image. To create RAW Image Select the given LINK.

http://www.hackingarticles.in/how-to-create-copy-of-suspects-evidence-using-ftk-imager

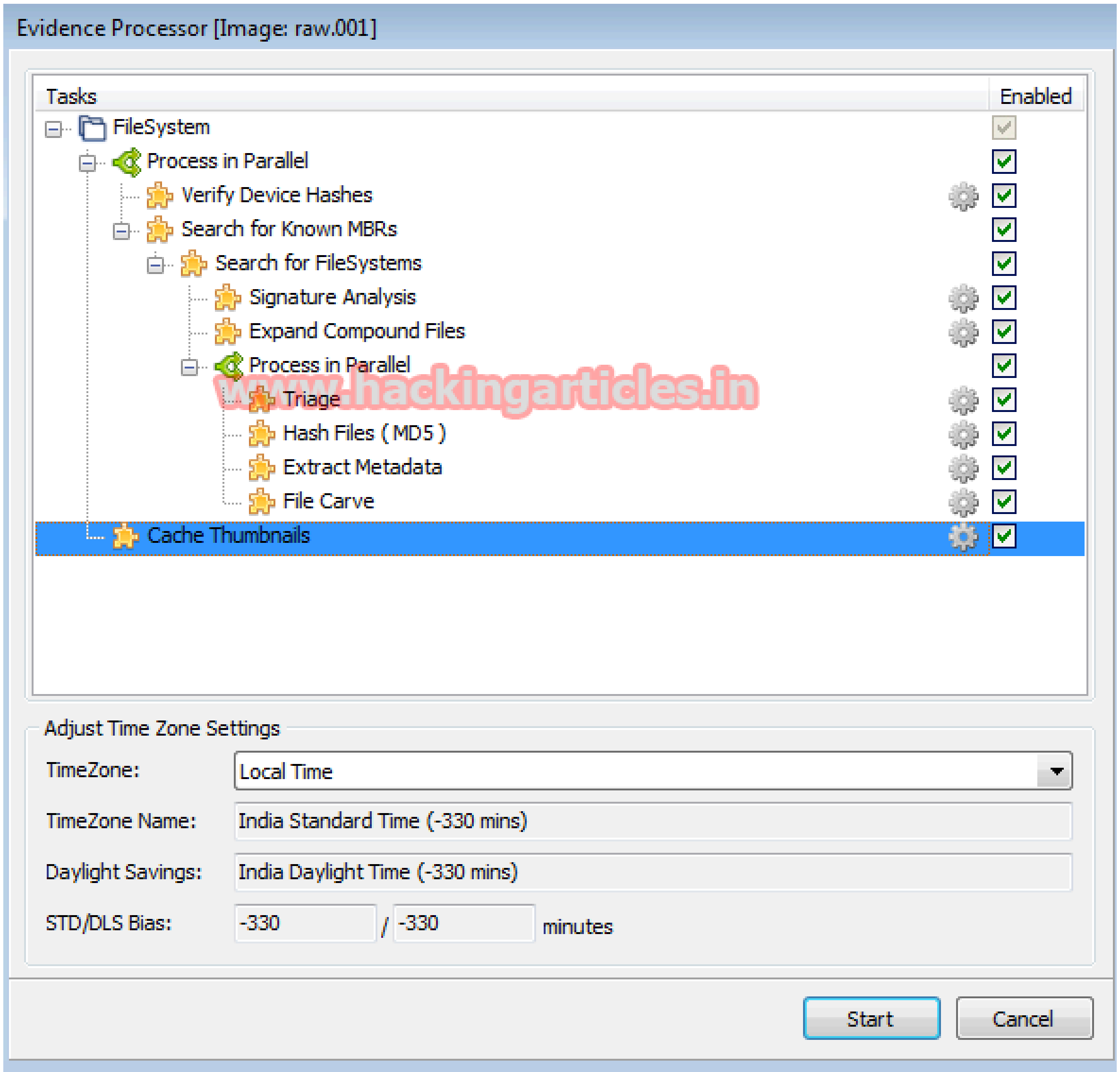


Name	Date modified	Type
raw.001	9/22/2015 2:40 PM	001 File

File name: raw.001

All Image Formats

Now Select tasks to be processed on RAW image from given list and click on Start.



Evidence Processor [Image: raw.001]

Tasks	Enabled
FileSystem	☑
Process in Parallel	☑
Verify Device Hashes	☑
Search for Known MBRs	☑
Search for FileSystems	☑
Signature Analysis	☑
Expand Compound Files	☑
Process in Parallel	☑
Triage	☑
Hash Files (MD5)	☑
Extract Metadata	☑
File Carve	☑
Cache Thumbnails	☑

Adjust Time Zone Settings

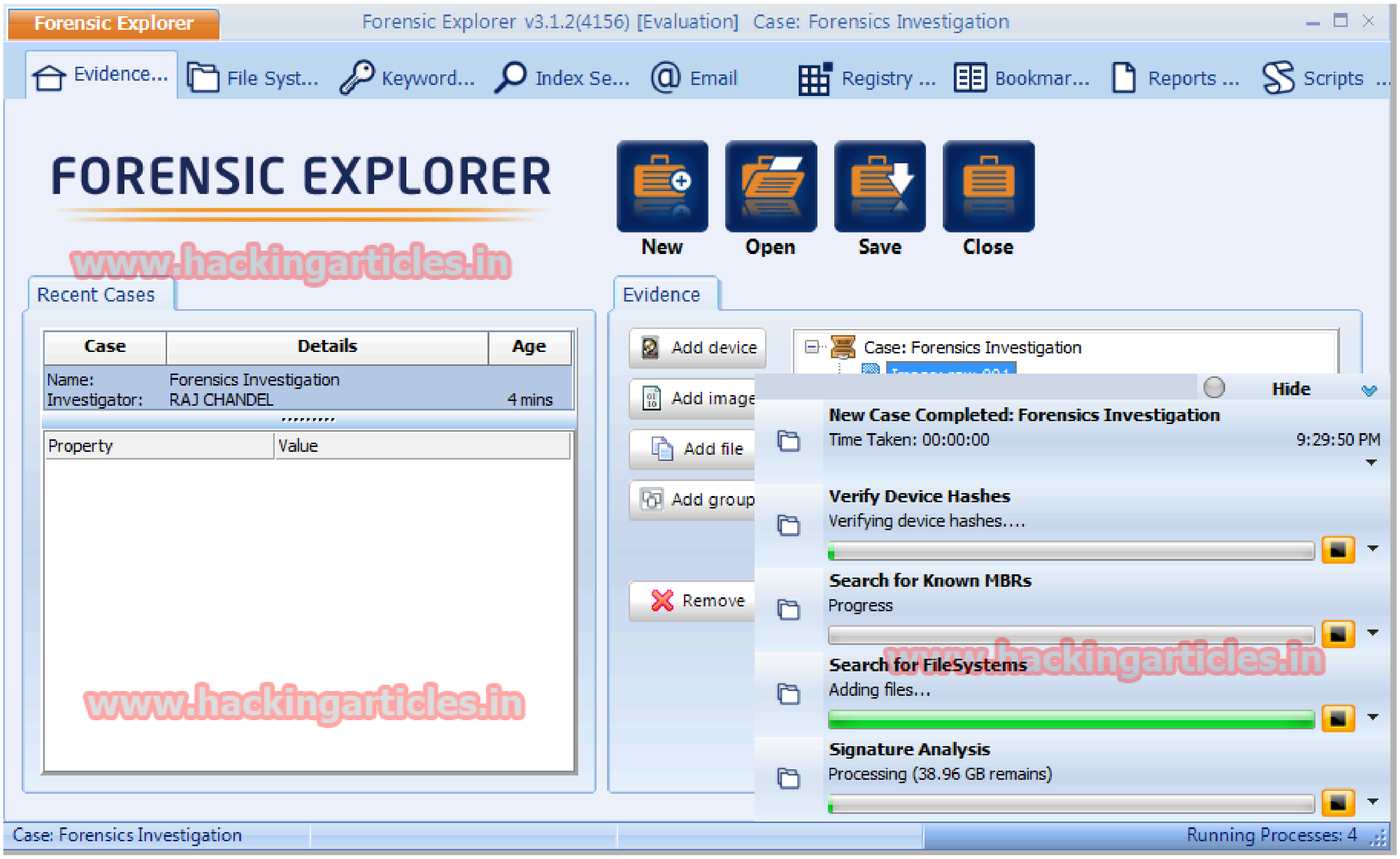
TimeZone: Local Time

TimeZone Name: India Standard Time (-330 mins)

Daylight Savings: India Daylight Time (-330 mins)

STD/DLS Bias: -330 / -330 minutes

After Process completion, it will show Result for all the tasks selected earlier.



Case	Details	Age
Name: Investigator:	Forensics Investigation RAJ CHANDEL	4 mins

Property	Value

Case: Forensics Investigation

New Case Completed: Forensics Investigation
Time Taken: 00:00:00 9:29:50 PM

Verify Device Hashes
Verifying device hashes....

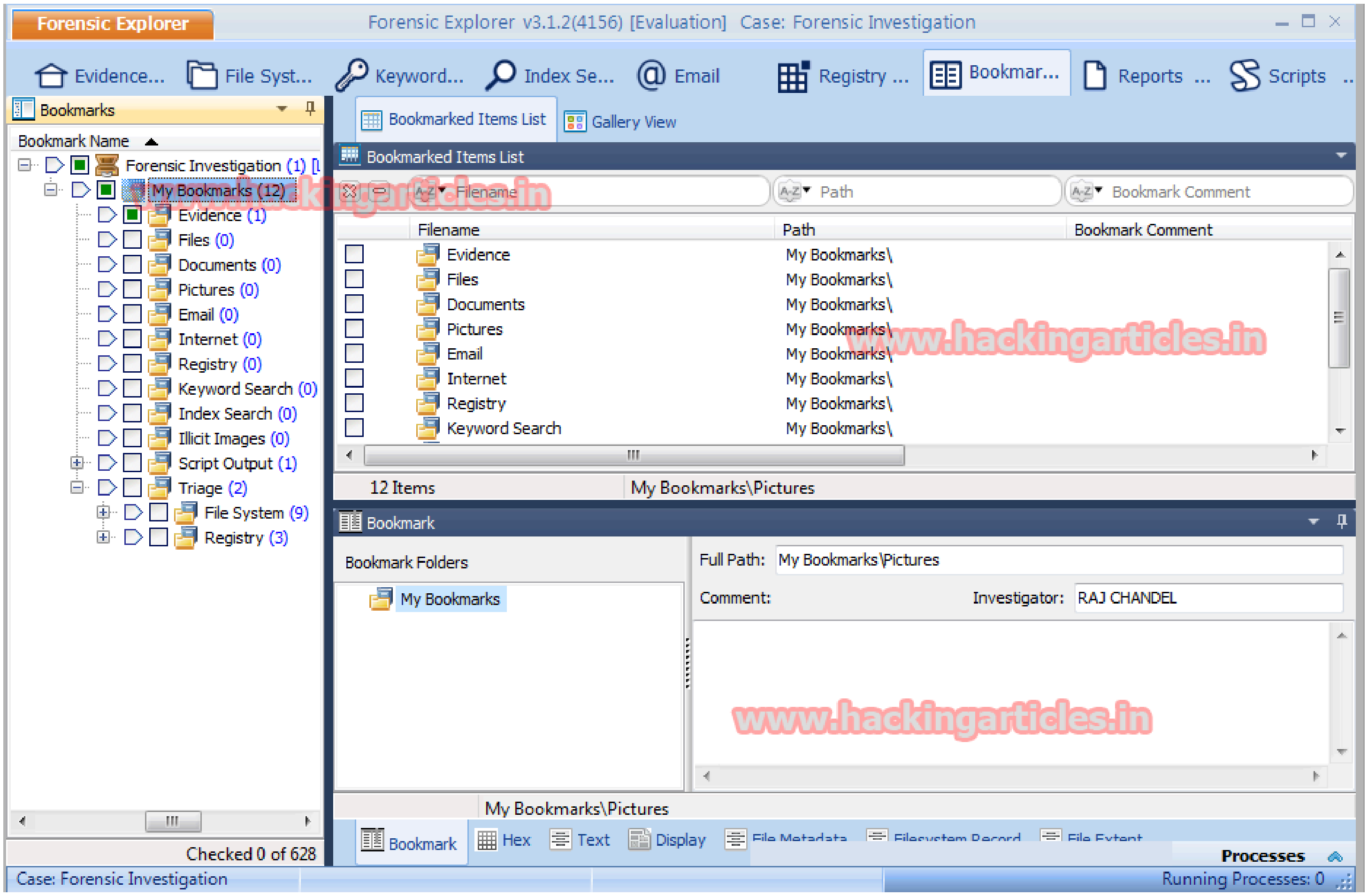
Search for Known MBRs
Progress

Search for FileSystems
Adding files...

Signature Analysis
Processing (38.96 GB remains)

Case: Forensics Investigation Running Processes: 4

Now Click on File System. The File System module is the primary Forensic Explorer window where actions such as **highlighting**, **selecting**, **sorting**, **filtering**, **flagging**, **exporting** and **opening** occur.



Bookmark Name

- Forensic Investigation (1)
  - My Bookmarks (12)
    - Evidence (1)
    - Files (0)
    - Documents (0)
    - Pictures (0)
    - Email (0)
    - Internet (0)
    - Registry (0)
    - Keyword Search (0)
    - Index Search (0)
    - Illicit Images (0)
    - Script Output (1)
    - Triage (2)
      - File System (9)
      - Registry (3)

Checked 0 of 628

Bookmarked Items List

	Filename	Path	Bookmark Comment
□	Evidence	My Bookmarks\	
□	Files	My Bookmarks\	
□	Documents	My Bookmarks\	
□	Pictures	My Bookmarks\	
□	Email	My Bookmarks\	
□	Internet	My Bookmarks\	
□	Registry	My Bookmarks\	
□	Keyword Search	My Bookmarks\	

12 Items My Bookmarks\Pictures

Bookmark

Bookmark Folders: My Bookmarks

Full Path: My Bookmarks\Pictures

Comment:

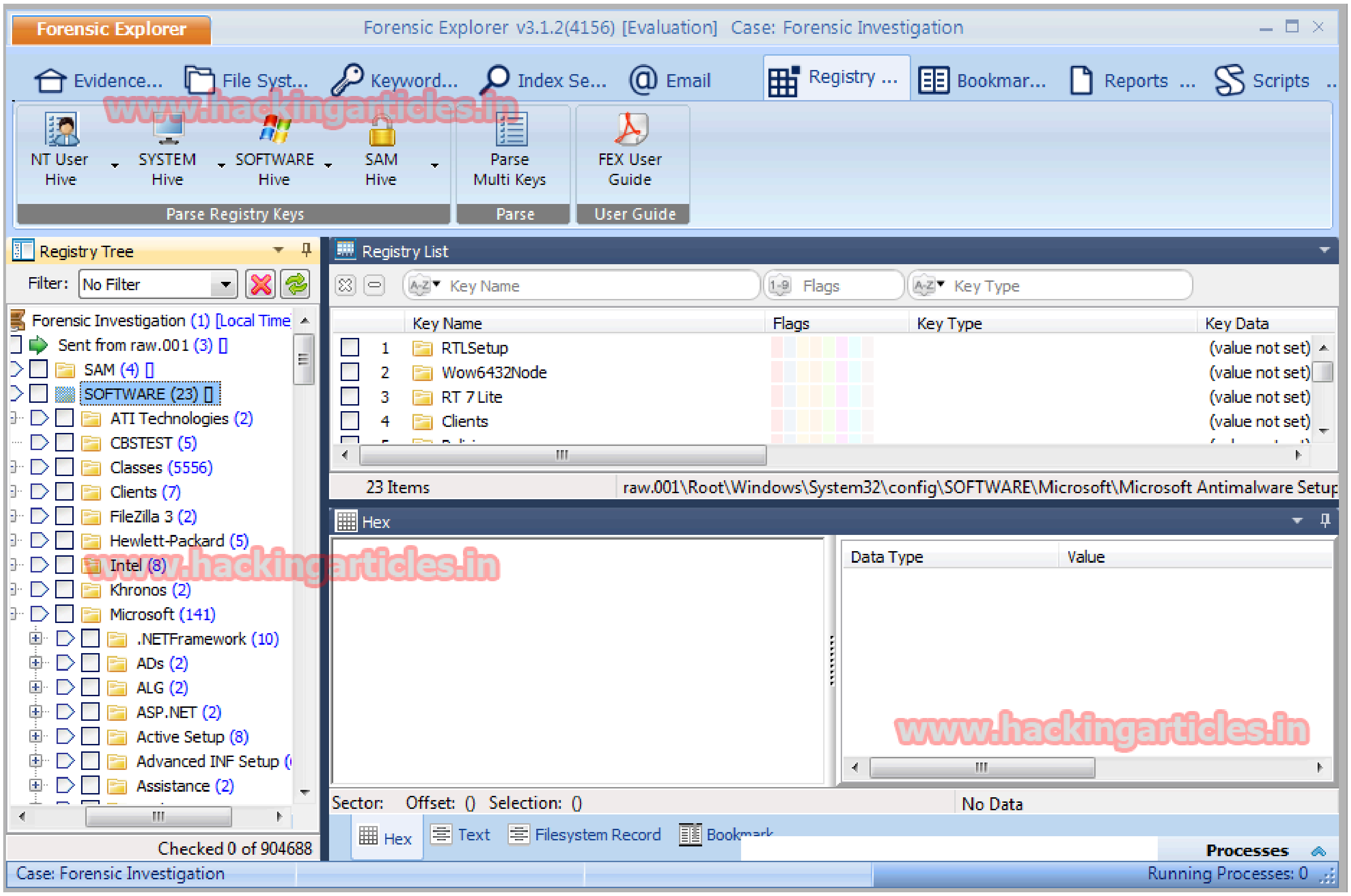
Investigator: RAJ CHANDEL

My Bookmarks\Pictures

Case: Forensic Investigation

Running Processes: 0

Select Registry analysis: Open and examine Windows registry hives. Filter, categorize and keyword search registry keys. Automate registry analysis with RegEx scripts.



Filter: No Filter

- Forensic Investigation (1) [Local Time
- Sent from raw.001 (3)
- SAM (4)
- SOFTWARE (23)
  - ATI Technologies (2)
  - CBSTEST (5)
  - Classes (5556)
  - Clients (7)
  - FileZilla 3 (2)
  - Hewlett-Packard (5)
  - Intel (8)
  - Khronos (2)
  - Microsoft (141)
    - .NETFramework (10)
    - ADs (2)
    - ALG (2)
    - ASP.NET (2)
    - Active Setup (8)
    - Advanced INF Setup (
    - Assistance (2)

Checked 0 of 904688

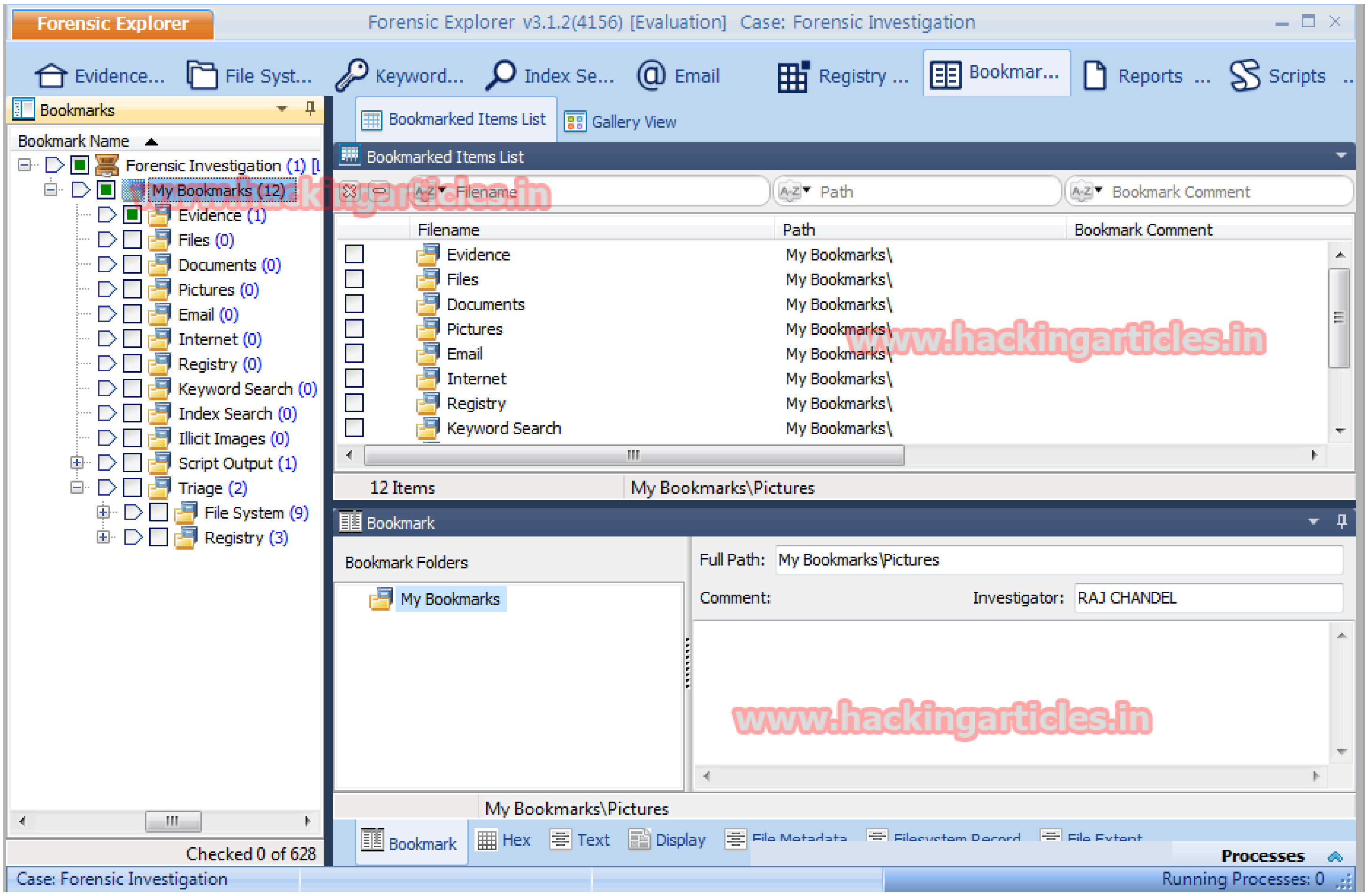
	Key Name	Flags	Key Type	Key Data
□ 1	RTLSetup			(value not set)
□ 2	Wow6432Node			(value not set)
□ 3	RT 7 Lite			(value not set)
□ 4	Clients			(value not set)

23 Items raw.001\Root\Windows\System32\config\SOFTWARE\Microsoft\Microsoft Antimalware Setup

Sector: Offset: () Selection: () No Data

Case: Forensic Investigation Running Processes: 0

Bookmark selection enables almost any item (e.g. file, folder, keyword, search hit, etc.), or a selection from an item (e.g. a fragment of text from a file or unallocated clusters), to be bookmarked and listed in the Bookmarks module.



Bookmark Name

- Forensic Investigation (1)
  - My Bookmarks (12)
    - Evidence (1)
    - Files (0)
    - Documents (0)
    - Pictures (0)
    - Email (0)
    - Internet (0)
    - Registry (0)
    - Keyword Search (0)
    - Index Search (0)
    - Illicit Images (0)
    - Script Output (1)
    - Triage (2)
      - File System (9)
      - Registry (3)

Checked 0 of 628

Bookmarked Items List

	Filename	Path	Bookmark Comment
□	Evidence	My Bookmarks\	
□	Files	My Bookmarks\	
□	Documents	My Bookmarks\	
□	Pictures	My Bookmarks\	
□	Email	My Bookmarks\	
□	Internet	My Bookmarks\	
□	Registry	My Bookmarks\	
□	Keyword Search	My Bookmarks\	

12 Items My Bookmarks\Pictures

Bookmark

Bookmark Folders: My Bookmarks

Full Path: My Bookmarks\Pictures

Comment:

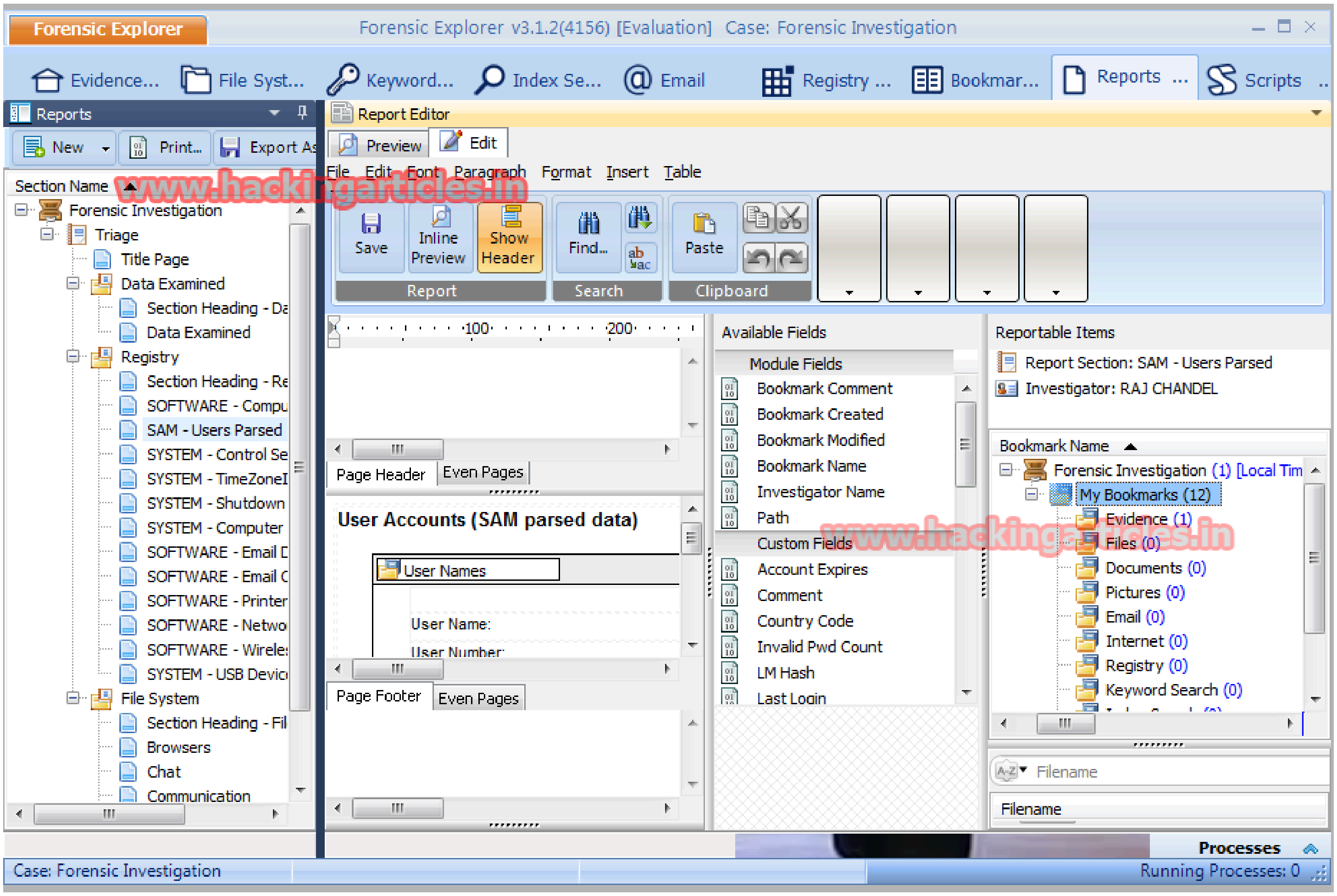
Investigator: RAJ CHANDEL

My Bookmarks\Pictures

Case: Forensic Investigation

Running Processes: 0

Reports: The purpose of the Reports Module is to assist in the generation of a report that documents the forensic analysis. The Reports module is based on the use of templates that can be re-used across multiple investigations.



Coming Soon Case Investigation and Analysis by Data Management, Keyword and Index Searching, Email Analysis , Registry Analysis & report creation using Forensic Explorer.