Forensic Investigation: Pagefile.sys

October 22, 2020 By Raj Chandel

In this article, we will learn how to perform a forensic investigation on a Page File. There is a lot of information that can be extracted from valuable artifacts through a memory dump. Yet, there is more: you can perform memory forensics even without a memory dump that is by virtual memory analysis.

There are records on the drive that contain a few pieces of memory. These files are pagefile.sys, swapfile.sys, and hiberfil.sys. We will be moving forward with pagefile.sys.

Table of Contents

Introduction

The Pagefile.sys also referred to as a swap file or virtual memory file is utilized inside Windows operating frameworks to store information from the RAM when it turns out to be full. The pagefile.sys in Windows operating framework is located at C:\pagefile.sys. Windows OS supports up to 16 paging files; only one is used currently.

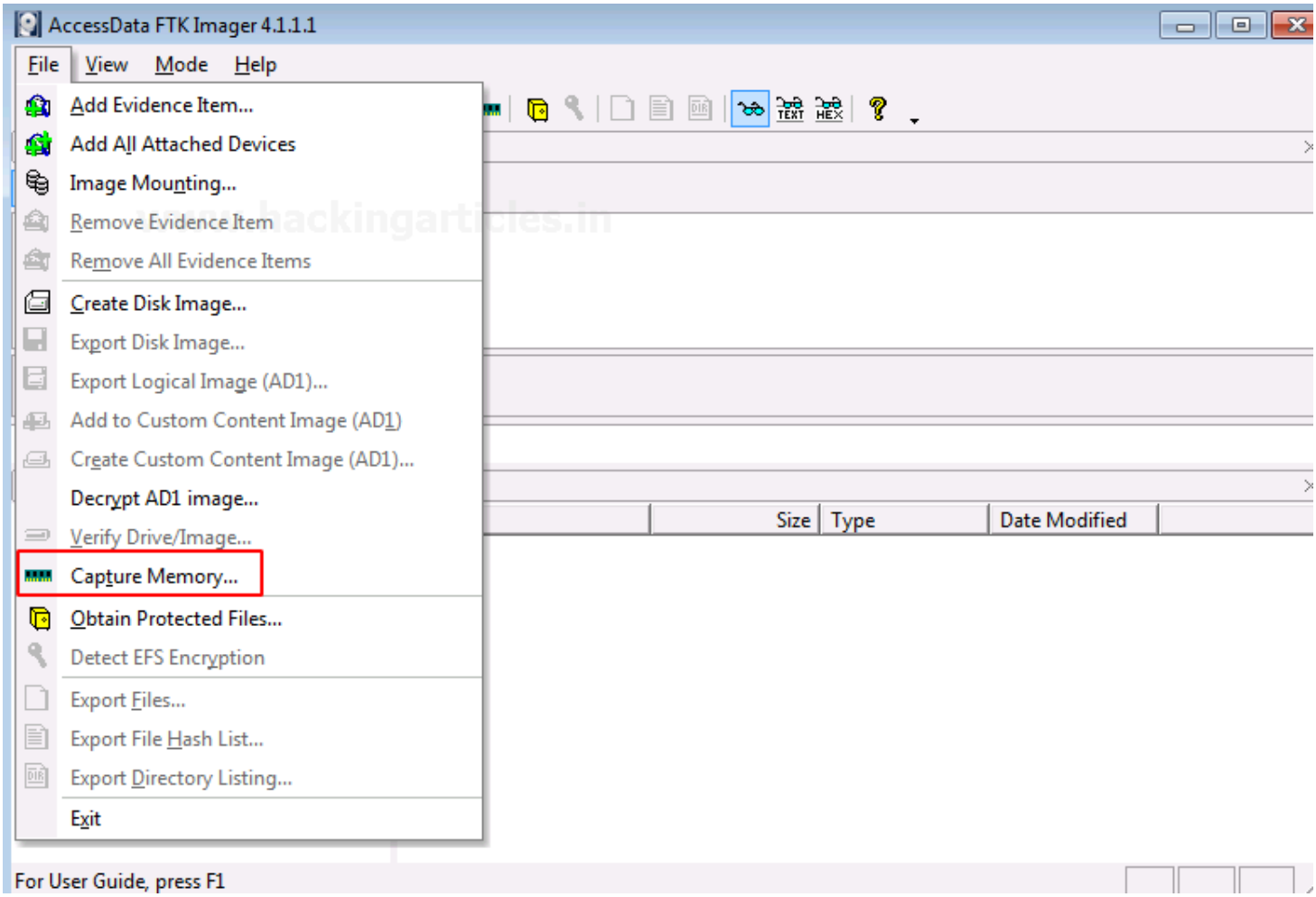
At whatever point you open an application in Windows, your PC will consume RAM. At the point when you have more applications open than the RAM on your PC can deal with, programs previously running in the RAM are moved to the Page file. This is known as Paging and implies the Page file goes about as reinforcement RAM, also known as virtual memory.

Capturing the memory and pagefile using FTK Imager

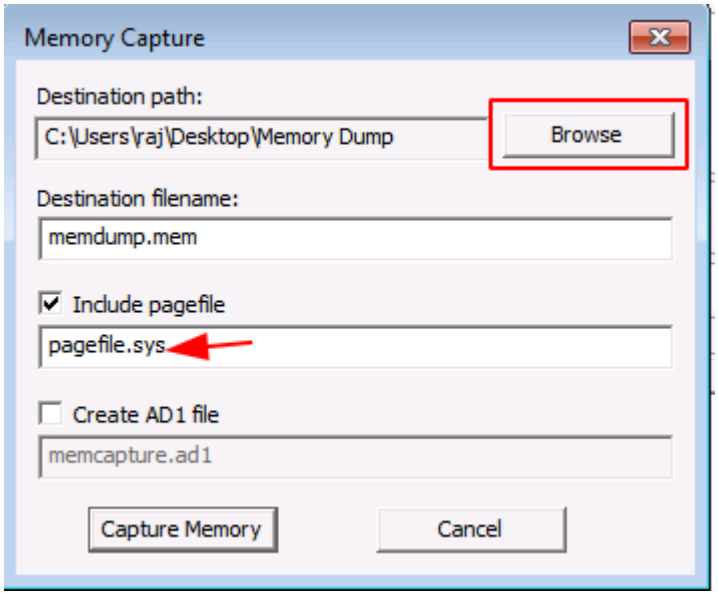
We will use **FTK Imager** to capture the memory along with the pagefile.sys.

FTK® Imager is a tool for imaging and data preview FTK Imager also create perfect copies (forensic images) of computer data without making changes to the original evidence. You can download FTK imager from **here**.

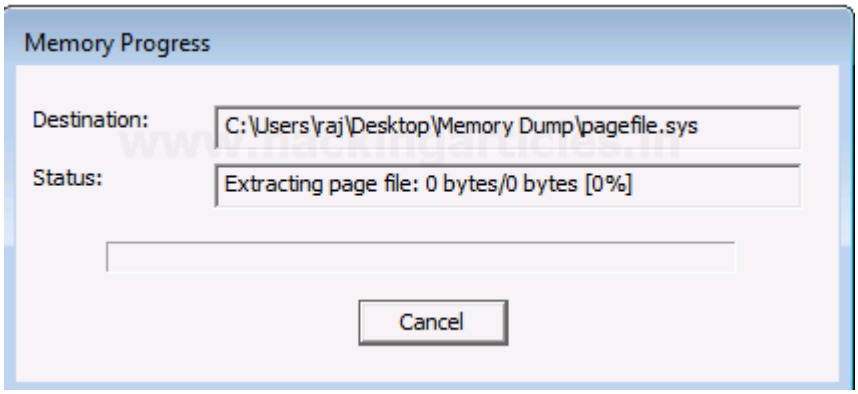
Click on **capture memory** to create a memory dump.



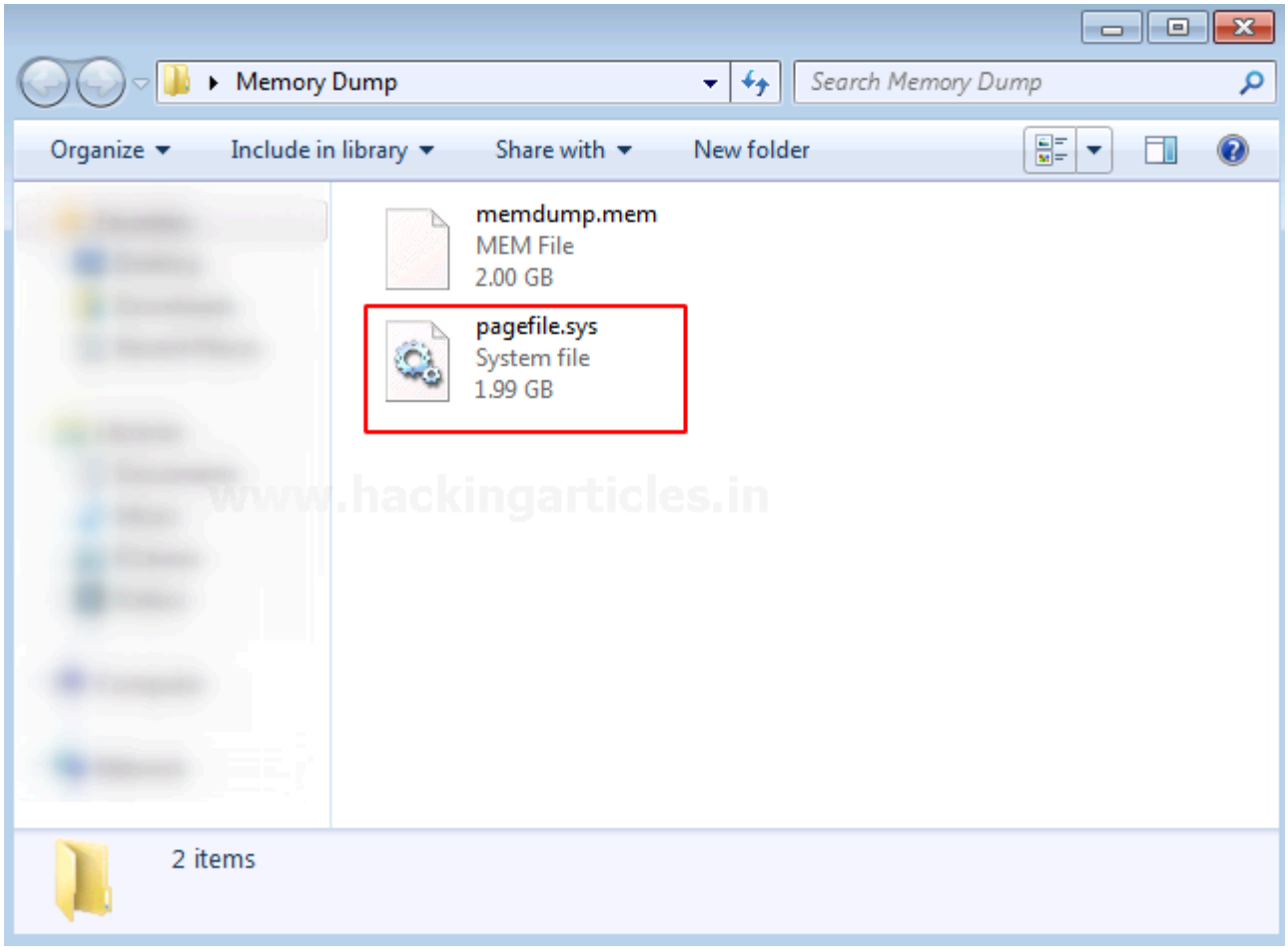
The next step is to browse the destination path as you like, select the alternative “include pagefile” and click on Capture Memory.



The memory capture process will begin once you click on capture memory.



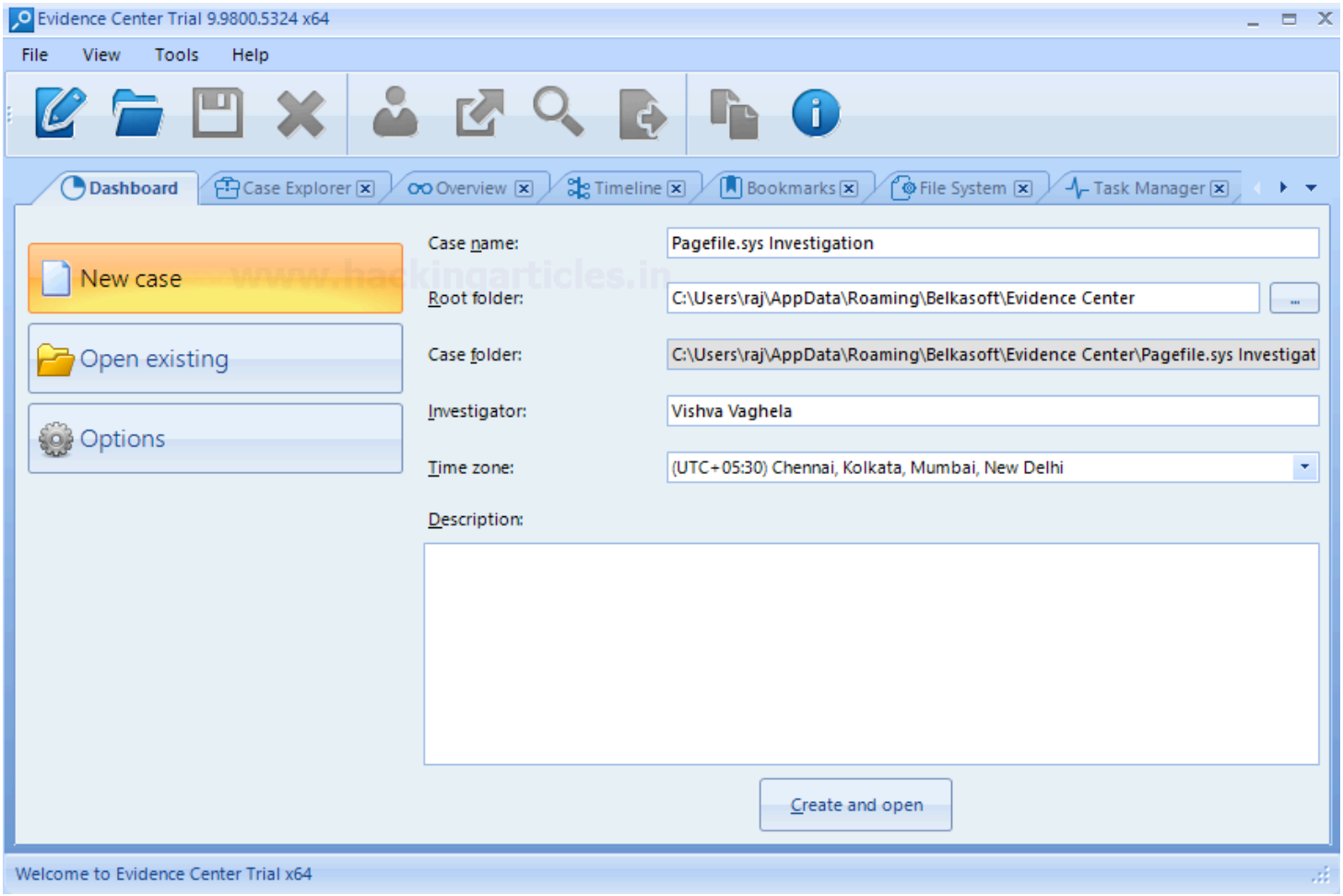
After completion of the process, the memory dump and page file will be carved in the destination folder previously selected.



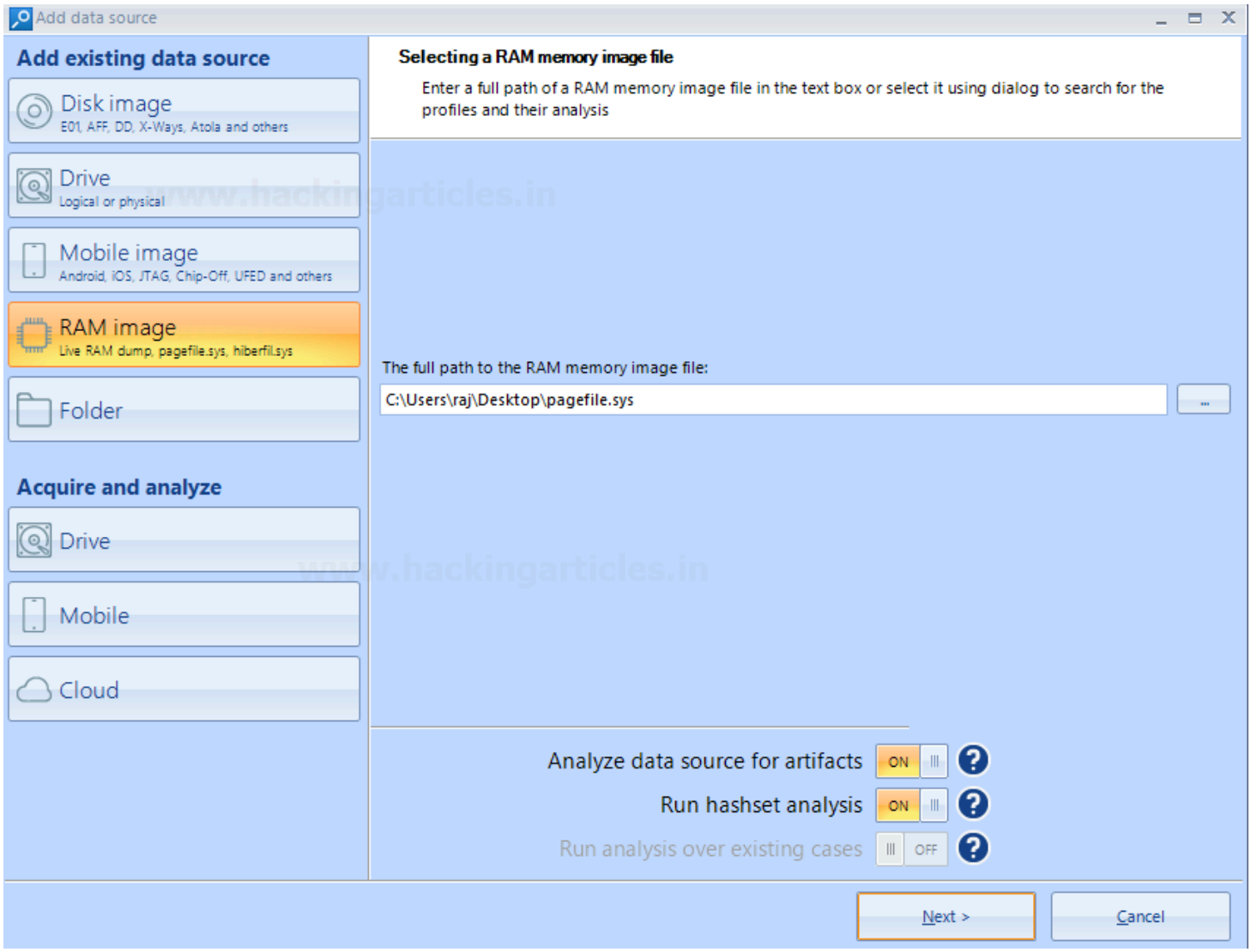
Analyzing using Belkasoft Evidence Centre

Now to analyze the carved file we will be using the tool, Belkasoft Evidence Centre for analysis of the pagefile.sys. Belkasoft Evidence Centre is an all-in-one forensic tool for acquiring analyzing and carving digital evidence. You can download the free trial of the tool from **here**.

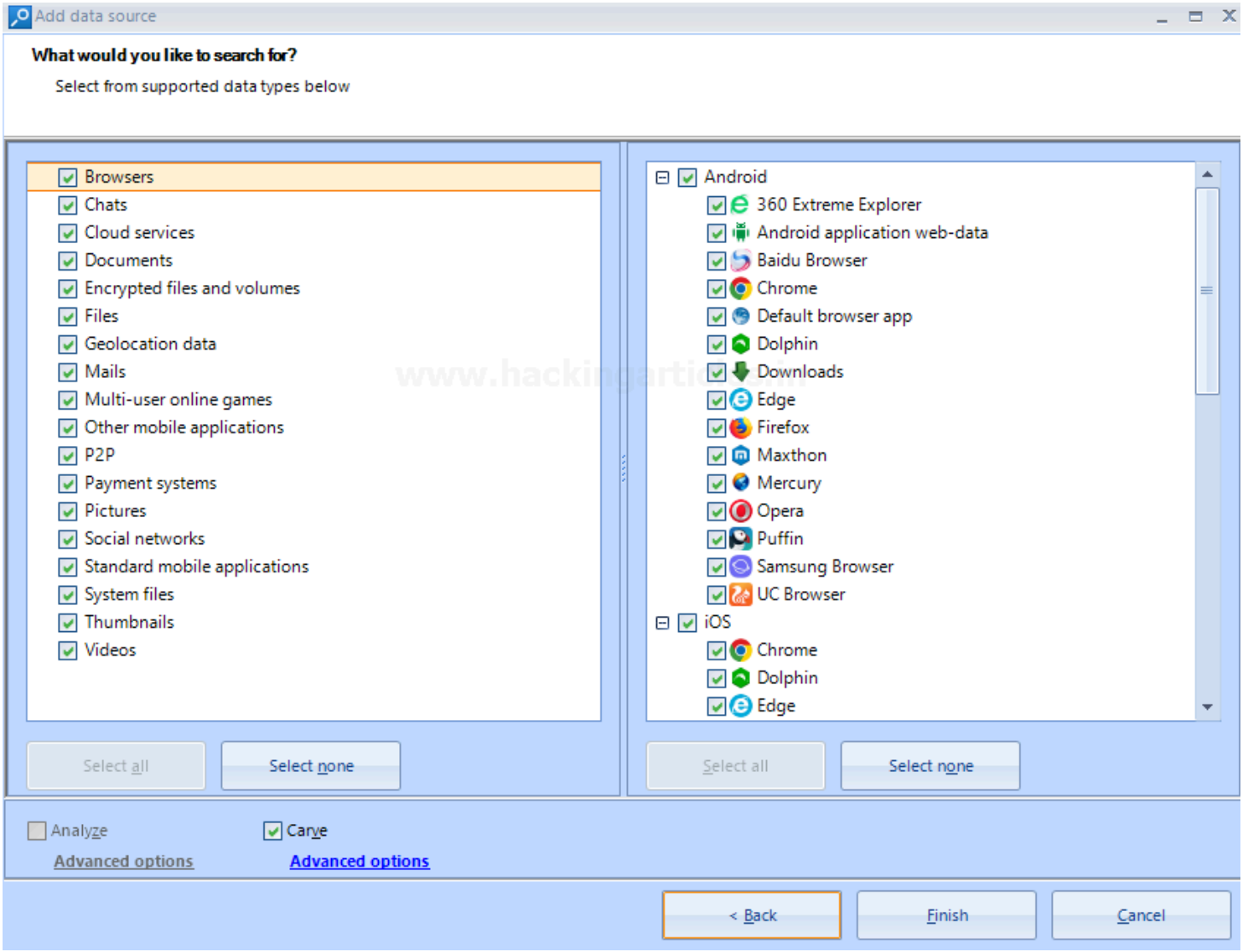
First of all, let's create a new case. Fill in the case information, select the root folder, if you want, you can add a case described as well. Click on create and open to proceed further with the analysis.



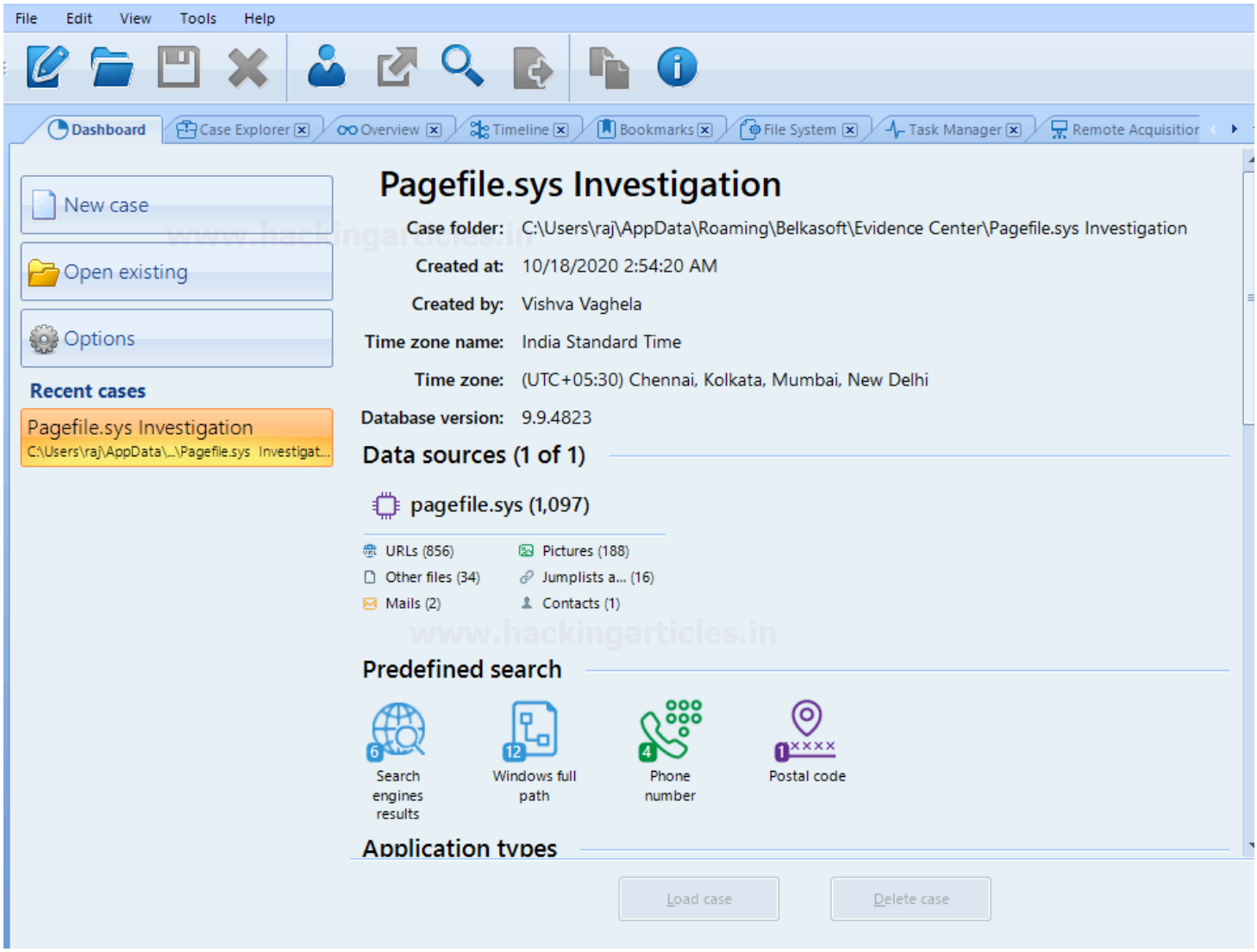
To analyze the captured memory (pagefile), select the option **RAM Image;** add the pagefile.sys file you carved previously as the evidence source using FTK imager.



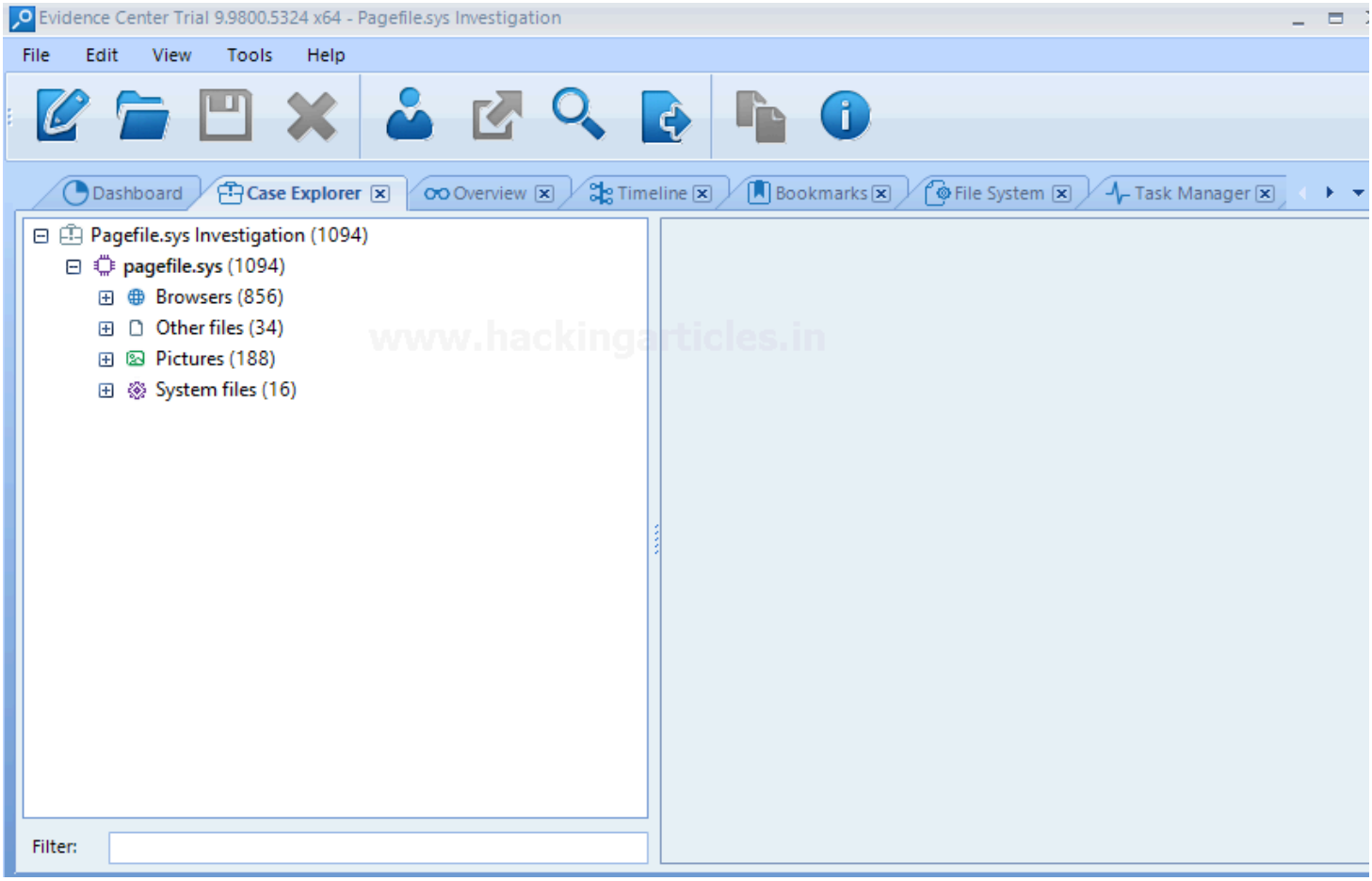
Choose the desired data type you would like to search for. There are a whole lot of data types supported by the tool. Click finish afterward.



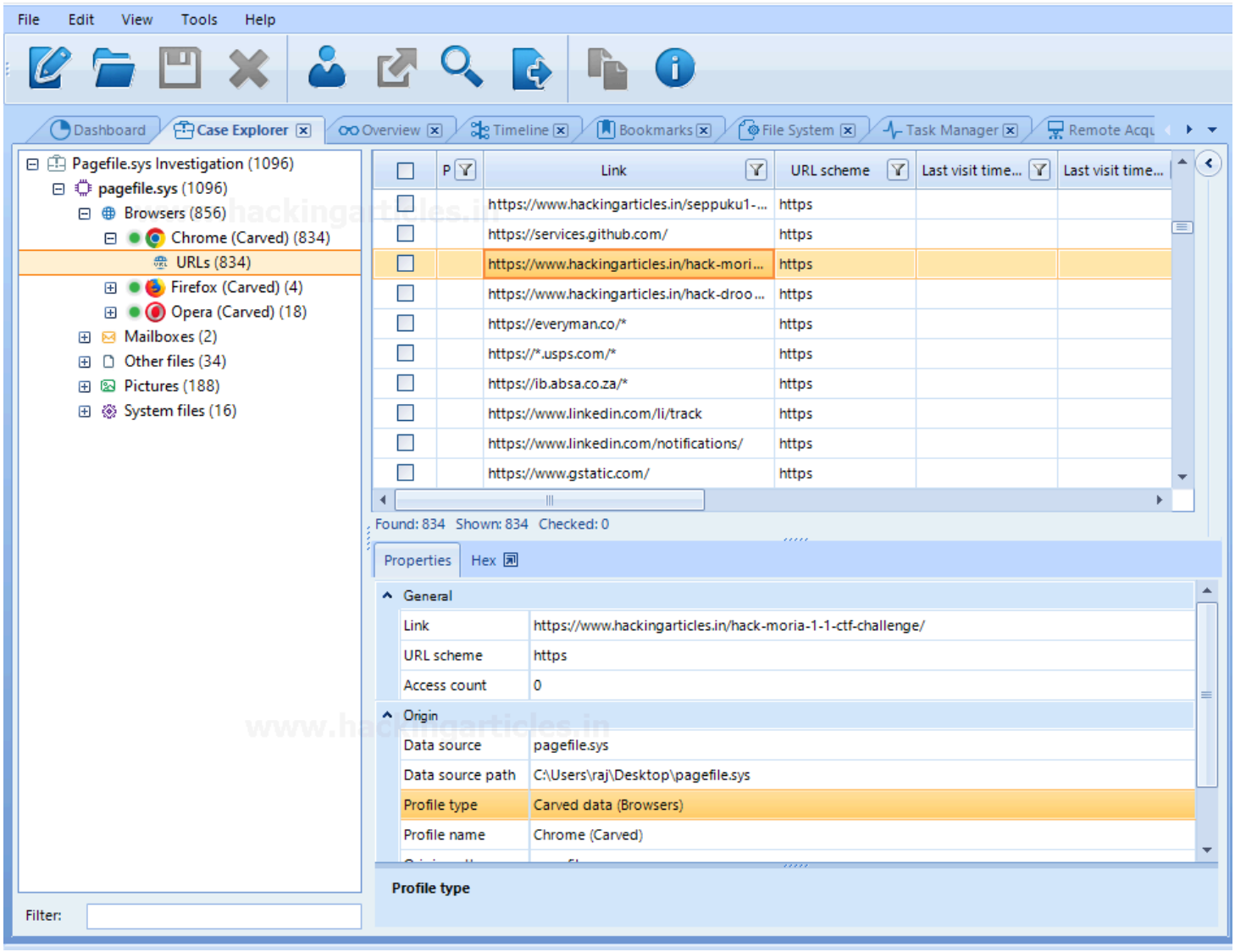
Here is the dashboard for the case after completion of the above steps. It shows proper segregated information about the data carved from the pagefile. A total of 1097 files have been carved, which includes URLs, pictures, and other artifacts.



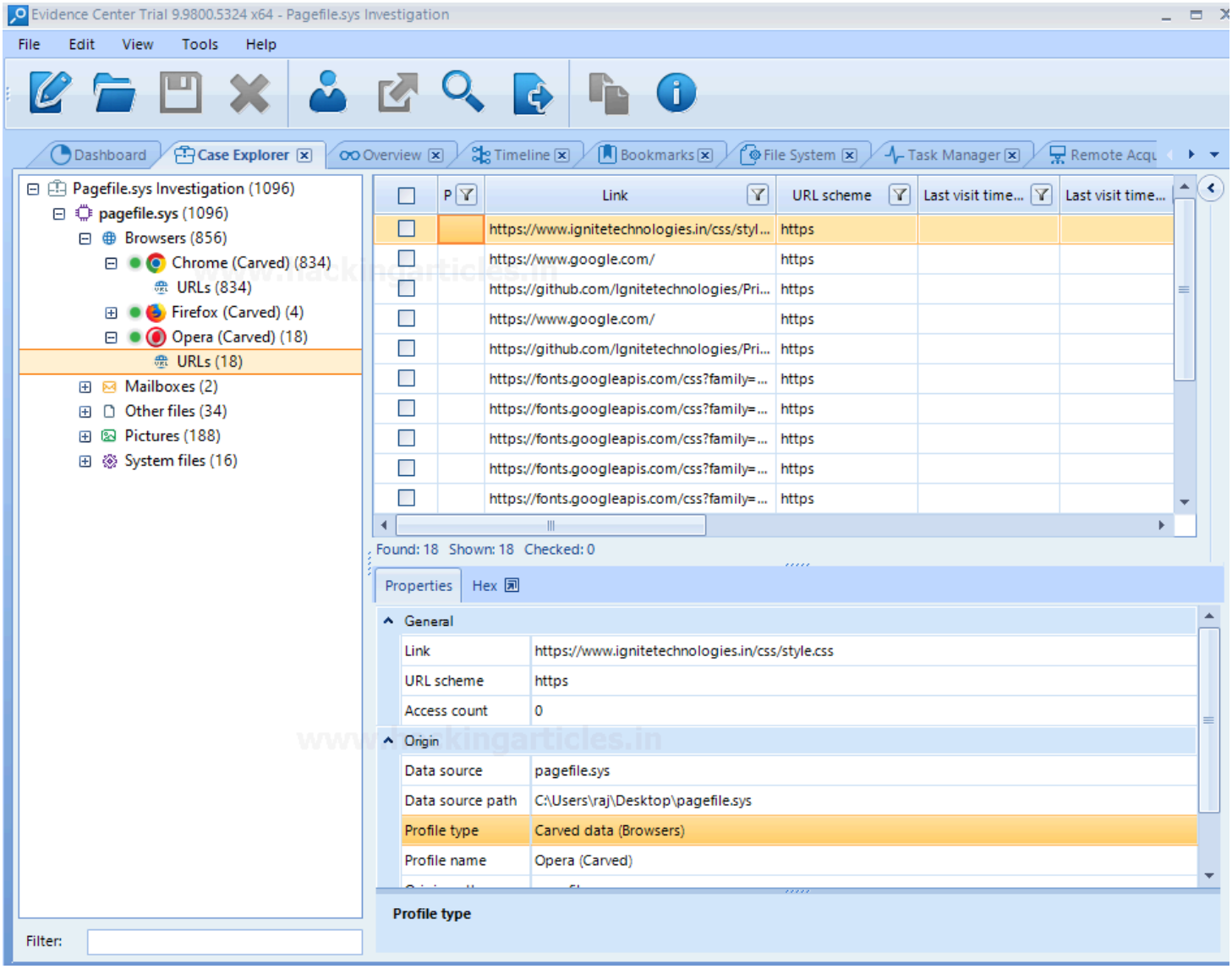
The case explorer tab right next to the dashboard tab allows expanding and viewing each profile column. The data has been carved from browsers, pictures, system files, and other files as well.



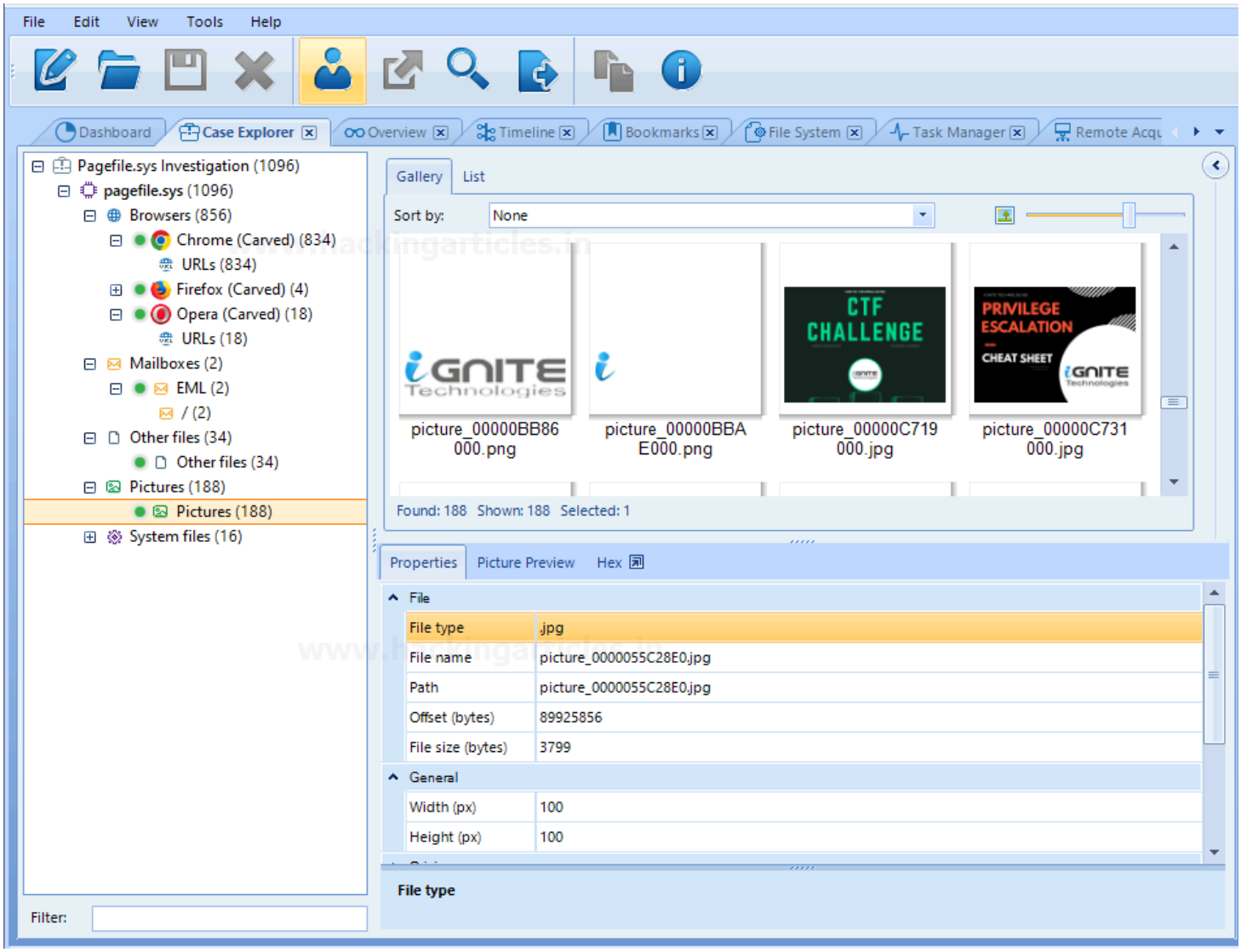
Let's expand and analyze the Browsers profile. It has carved the chrome history which consists of URLs, let's check the chrome carved section for more details. It consists of the URLs for the sites visited, one of which is highlighted in the following screenshot.



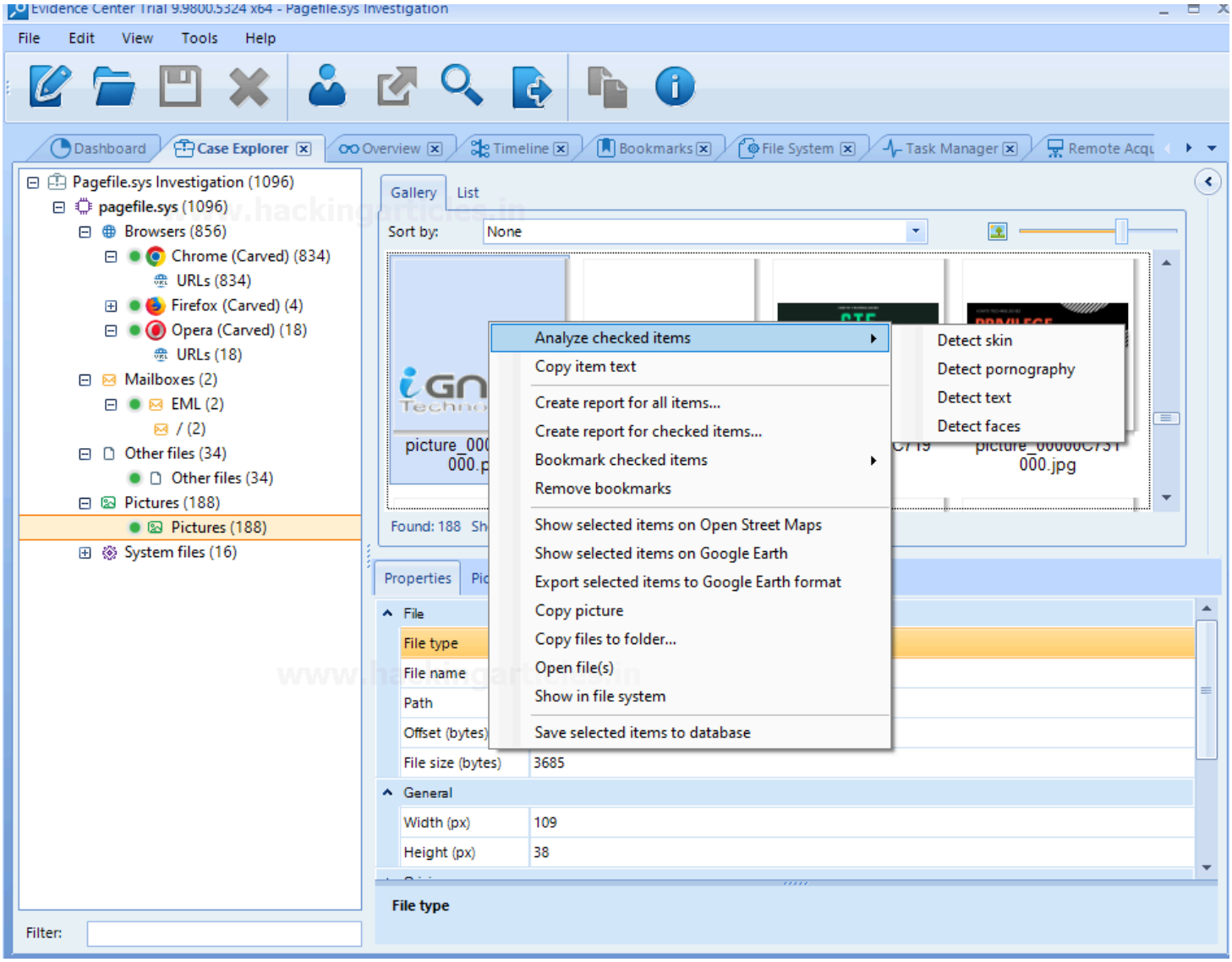
Another in browsers profile is opera. Analyze the opera(carved) profile similarly, shows details about the URLs visited.



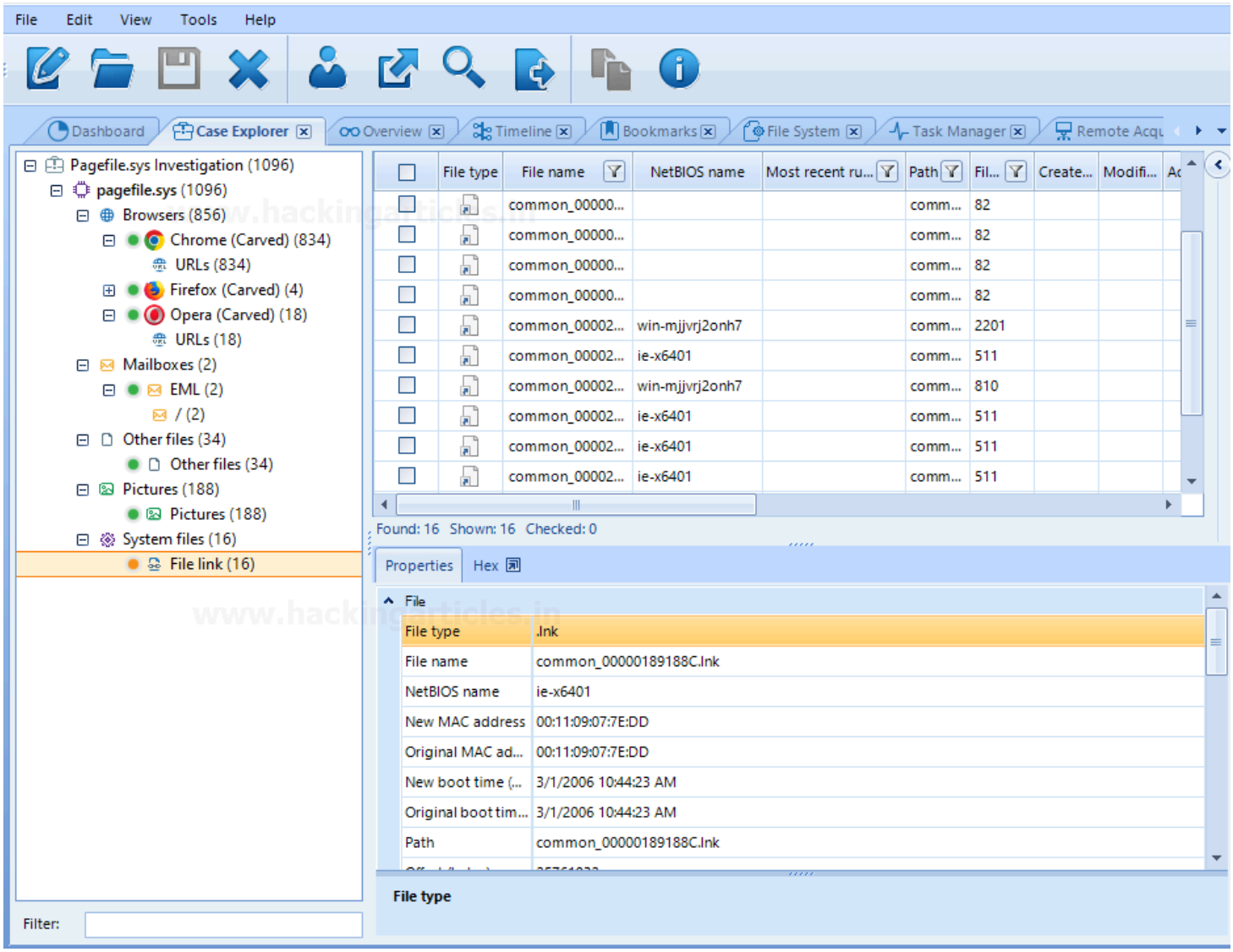
The carved data from pagefile also consists of some images. These images can be from the sites I have visited and other thumbnails.



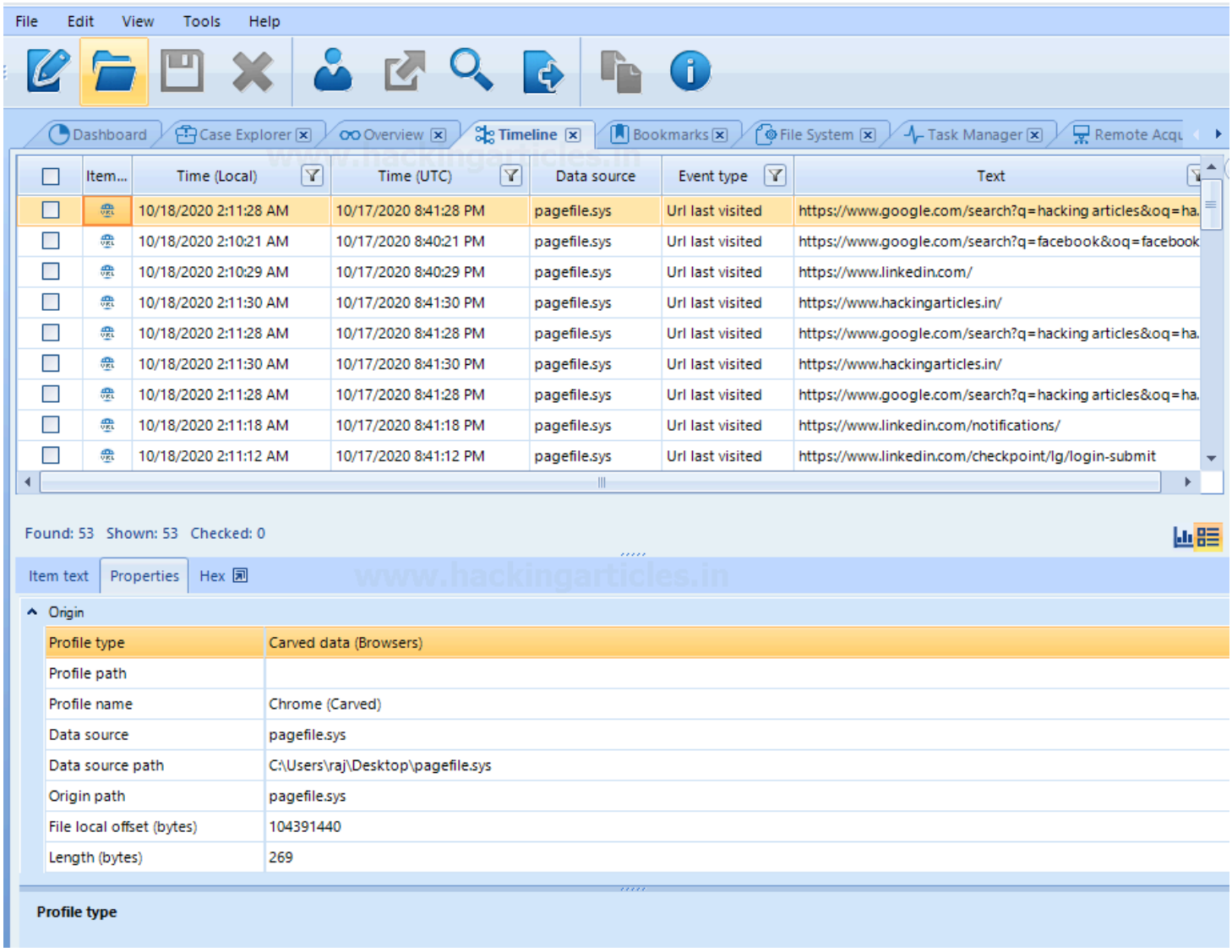
The great feature of the belkasoft evidence center is it allows you to simply right on the picture and analyzes it for various aspects such as check skin, detect pornographic content from the picture, detect text, and also faces. All these aspects are useful during live analysis.



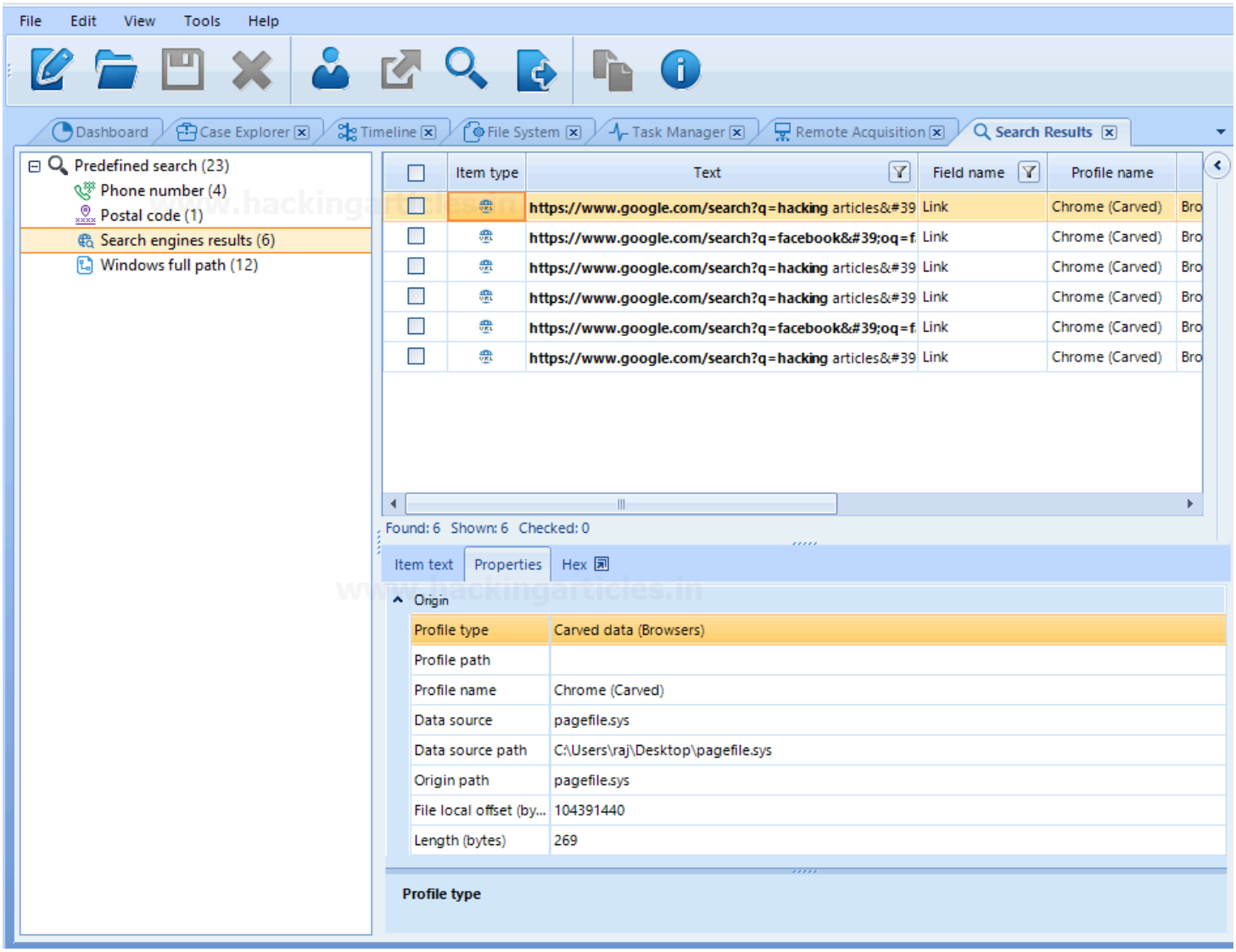
Some system files are also carved from the captured virtual memory, show the NetBIOS name, file path, and size.



The timeline tab shows the overall view of the data carved for easy analysis along with the time and URL of the search site visited.



A search results tab is also there in the tool which shows predefined search results. The following screenshot shows the search engine results along with the link and profile name.



Similarly, you can perform the forensic investigation for hiberfil. Export the hiberfil.sys (stores the data while the windows system is on Hibernate mode) using FTK located at C:/hiberfile.sys and further analyze it using Belkasoft Evidence Centre.

The analysis of virtual memory files serves a great purpose for web browser forensic.