【译】取证调查：虚拟内存pagefile.sys

2023-02-01 12:03:49

# 【译】取证调查：虚拟内存pagefile.sys

原文：<https://www.hackingarticles.in/forensic-investigation-pagefile-sys/>

在这片文章中，我们将学习如何在虚拟内存文件中进行取证调查。这里有很多信息能用于在内存镜像中提取有价值的信息。当然，更多的你还可以直接通过虚拟内存分析而不分析内存镜像。

在设备上有很多包含很多内存片段的记录。这些文件是pagefile.sys,swapfile.sys和hiberfil.sys。我们将对pagefile.sys进行分析。

## 目录

* 介绍
* 使用FTK imager获取内存和虚拟内存
* 使用Belkasoft Evidence Centre分析

## 介绍

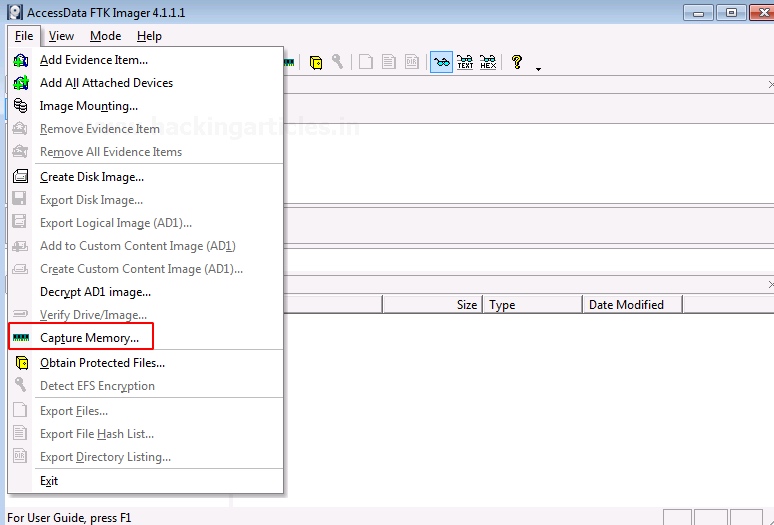
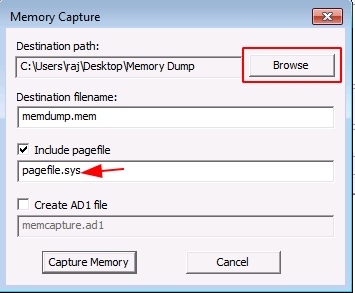
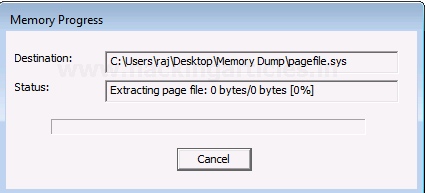
pagefile.sys也指在windows操作系统中被用于swap交换文件或者虚拟内存文件存储超出物理内存容量部分的信息。pagefile.sys在windows操作系统的位置位于 C:\pagefile.sys。windows操作系统最高支持16个分页文件；目前只有一个被使用。

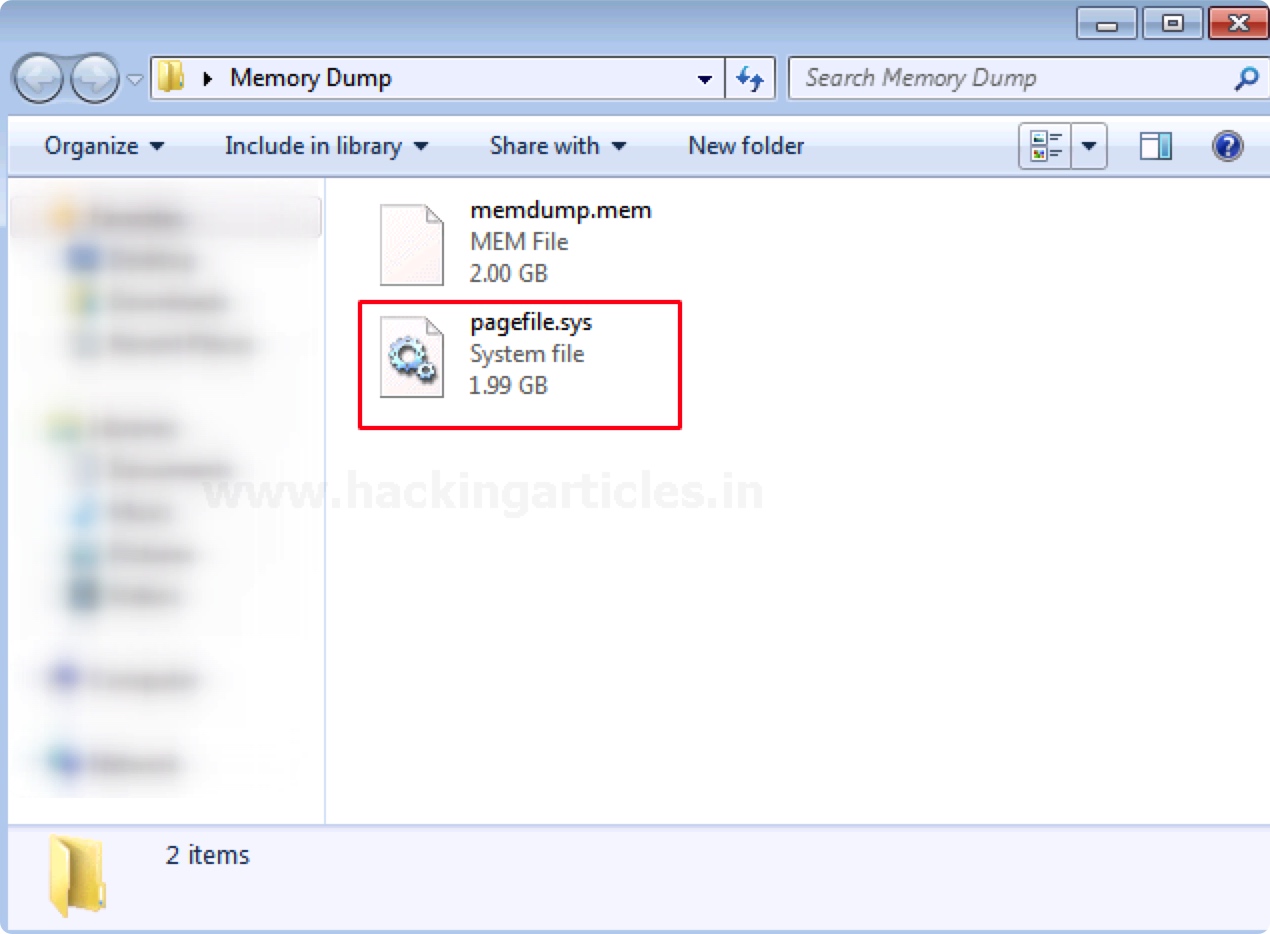
无论处于什么目的，当你在Windows中打开一个应用，你的PC将会用到RAM内存。当你打开更多的应用超出了PC内存能够容纳的范围，在内存中运行的程序将会被移动到虚拟内存中。这就是分页或者意味着分页文件被用作强化了内存，也被称为虚拟内存。

## 使用获取内存和虚拟内存

我们将使用FTK imager获取虚拟内存pagefile.sys。

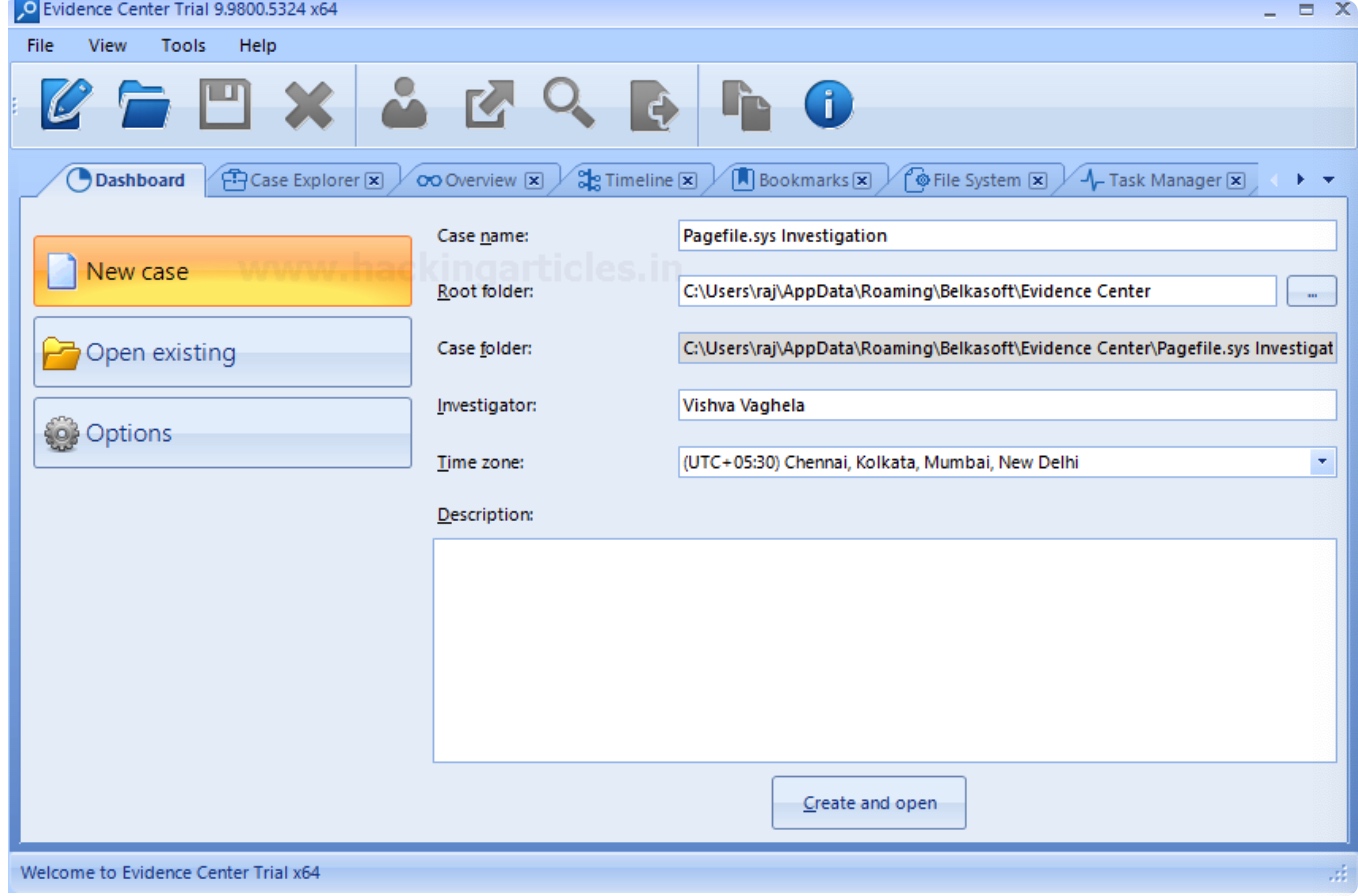
FTK imager是一个镜像和数据查看工具，FTK imager通常创建系统镜像（取证镜像）电子证据。你可以在这里下载FTK imager（<https://www.exterro.com/ftk-imager>）

点击capture memory创建内存镜像。  
  
下一步是选择保存的目录，勾选”include pagefile“，点击获取内存capture memory。  
  
内存获取进程将会在点击capture memory按钮之后开始。  


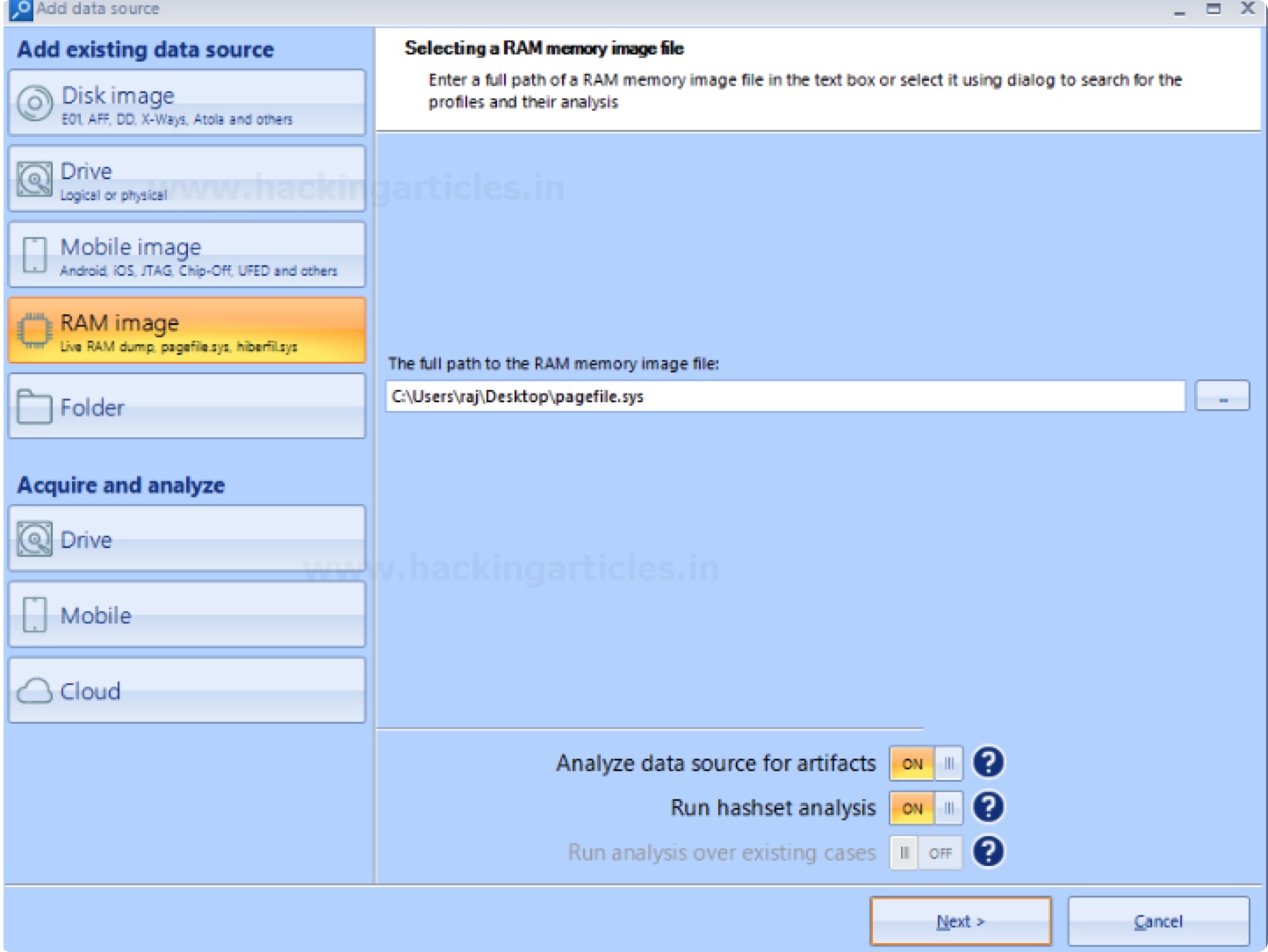
进程结束后，内存镜像和虚拟内存就会被写在之前选定的目录中。  


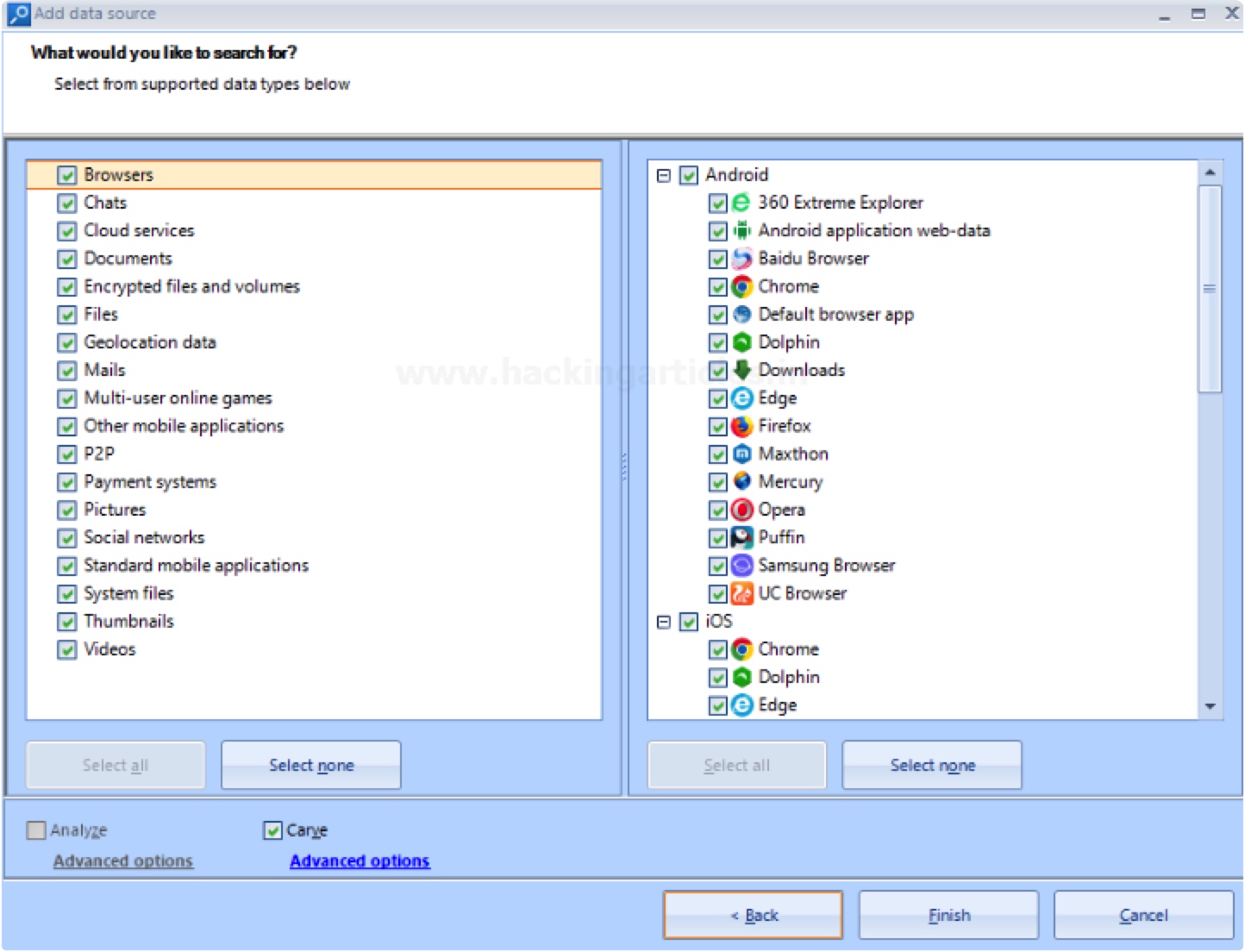
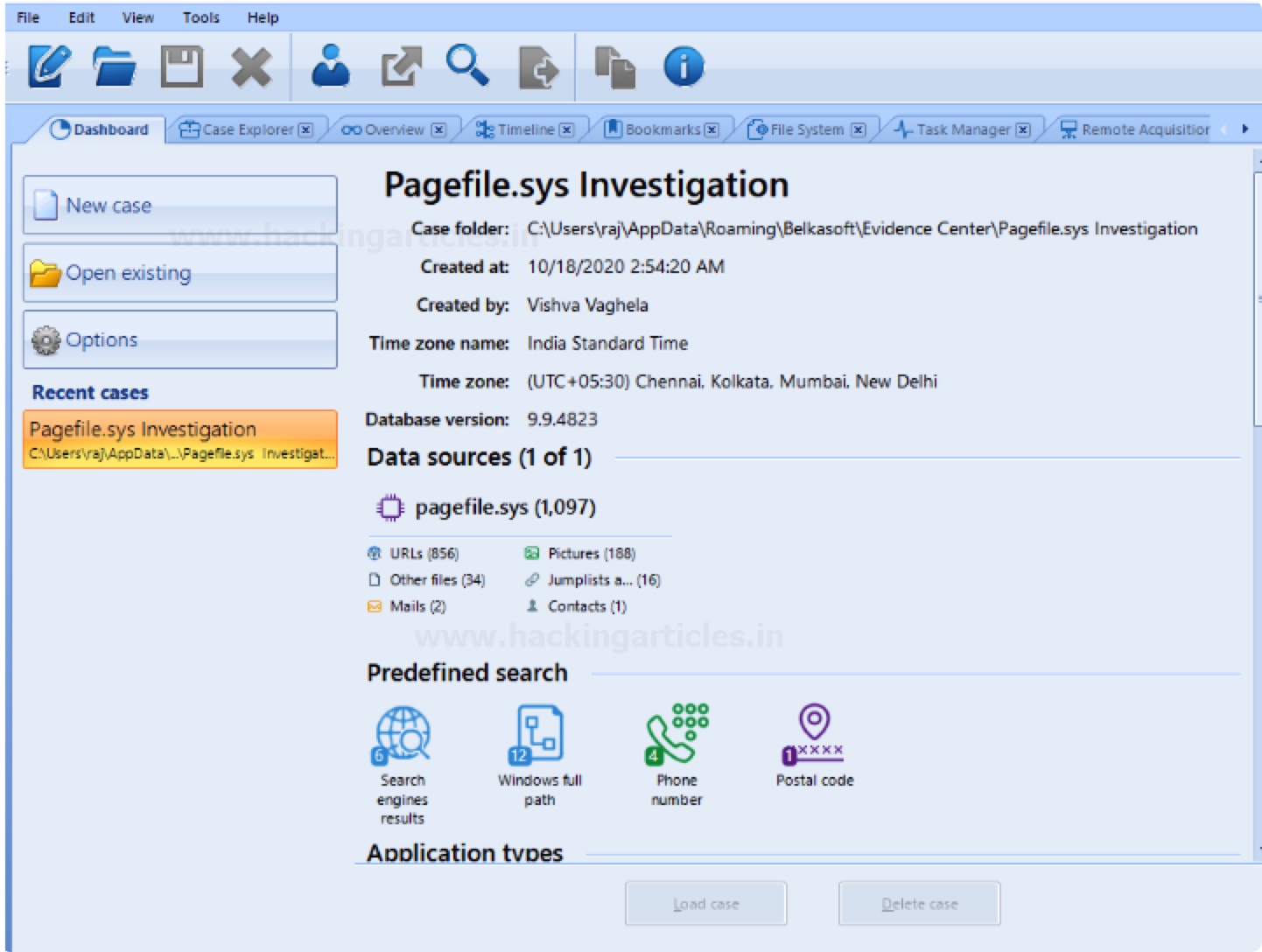
## 使用Belkasoft Evidence Centre分析

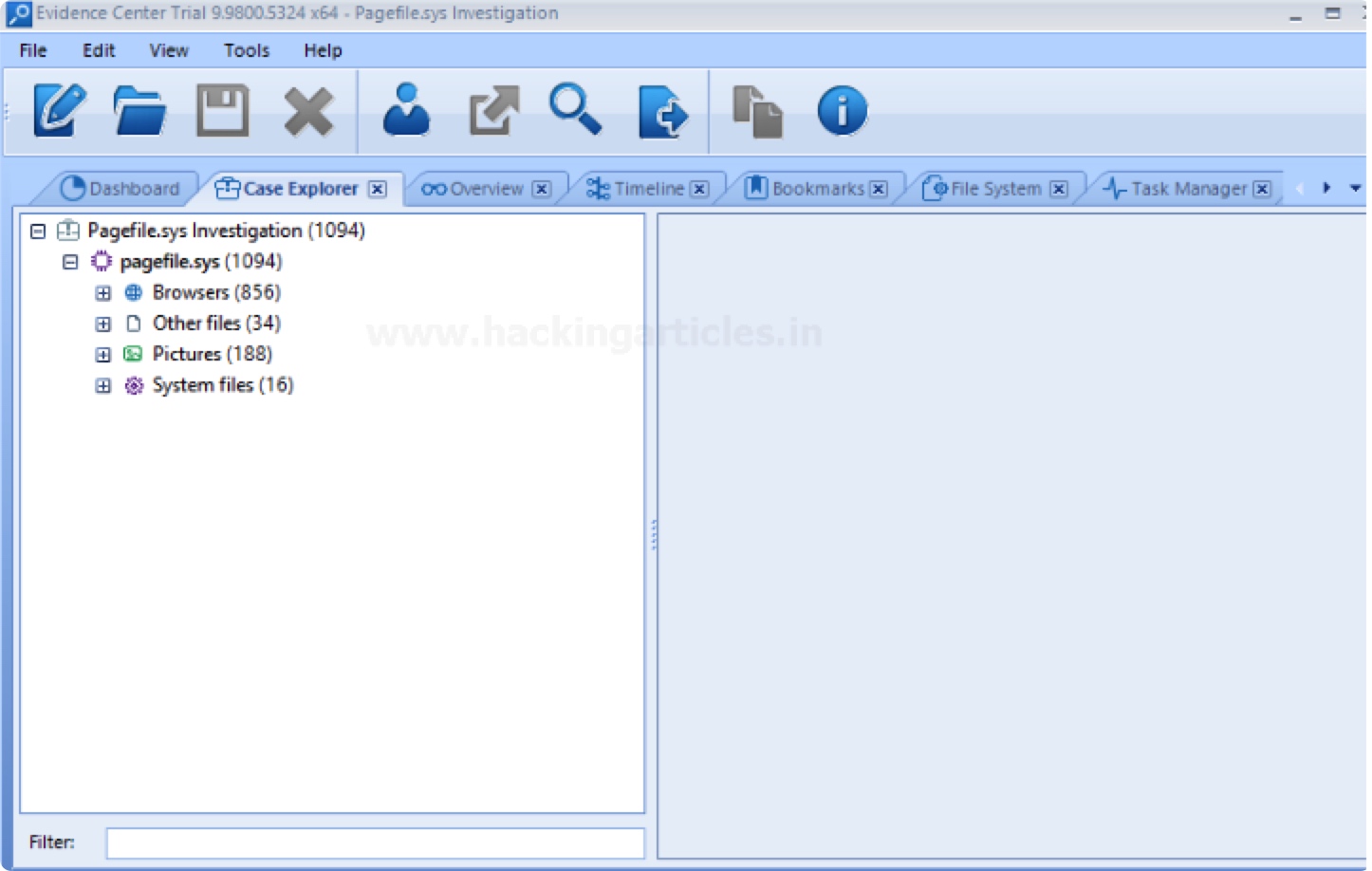
现在我们来Belkasoft Evidence Centre分析写入pagefile.sys。Belkasoft Evidence Centre是一个集成获取、分析和刻入数字证据的分析工具。你可以在这里下载免费版本的工具（<https://belkasoft.com/get>）

首先，我们创建个新的case。填写case信息，选择有管理权限的文件夹，如果你想的话，你还可以添加一个case的描述。点击“create and open”执行分析。  


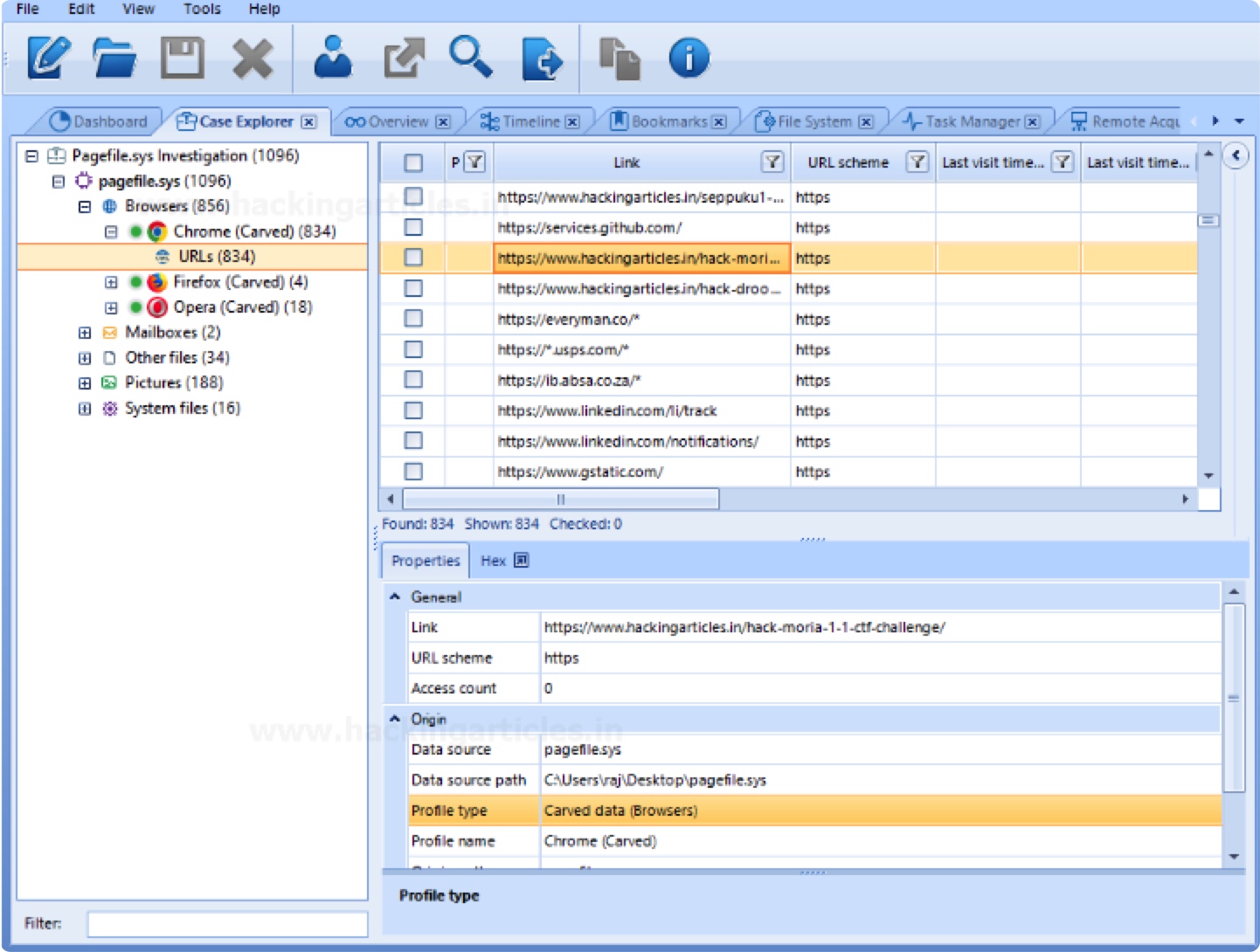
用于分析虚拟内存文件，选择配置RAM image内存镜像；添加使用FTK imager镜像的pagefile.sys文件。

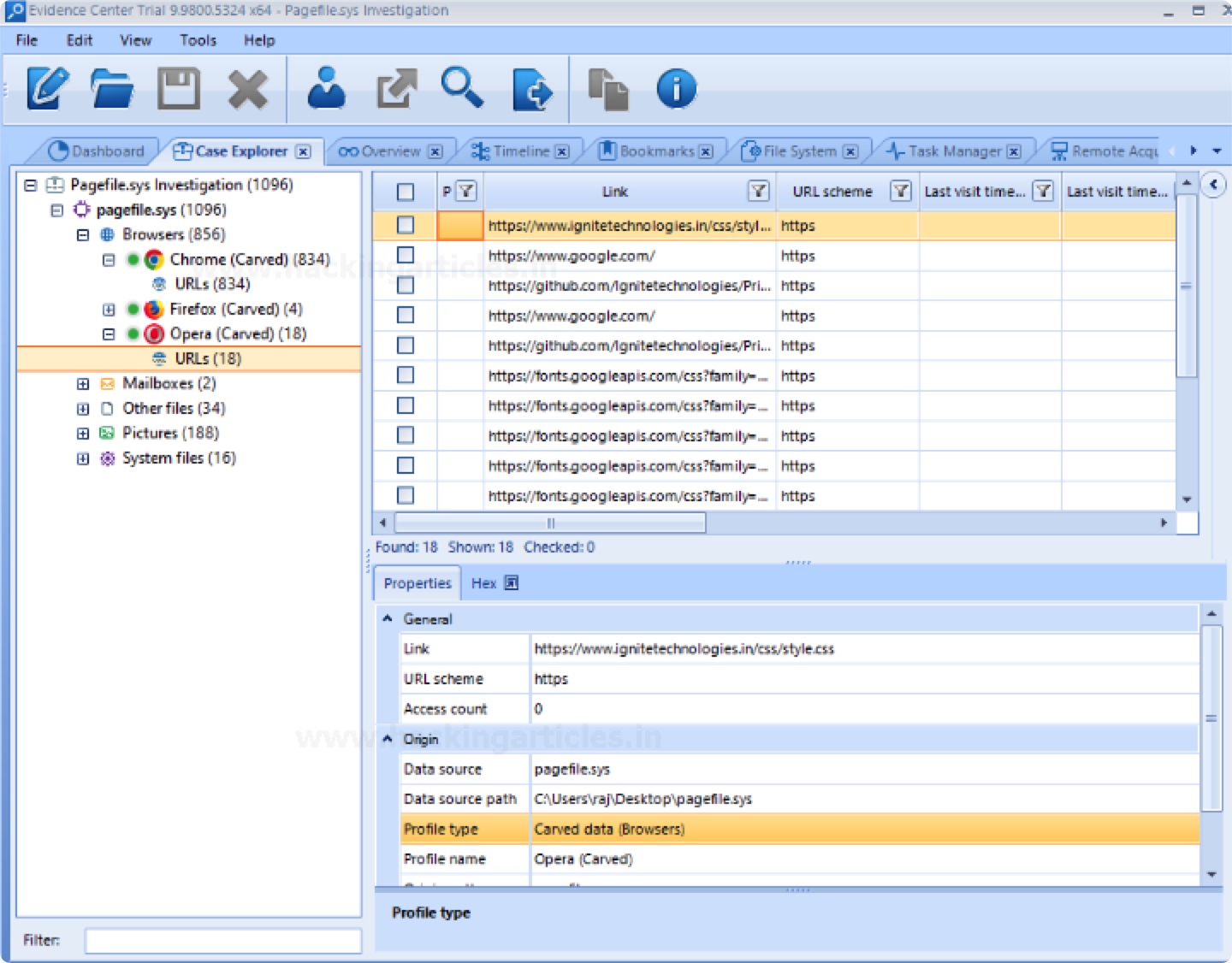
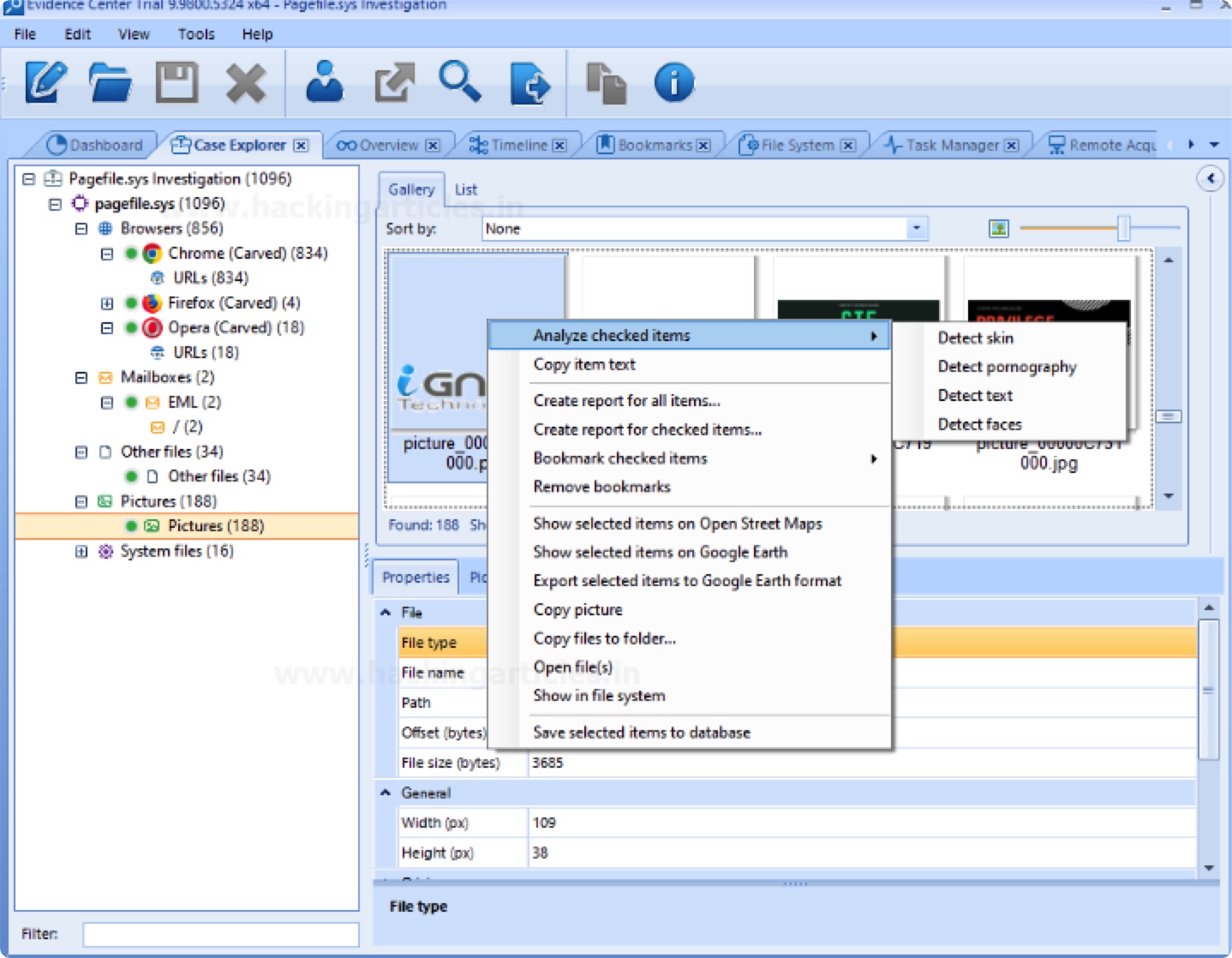
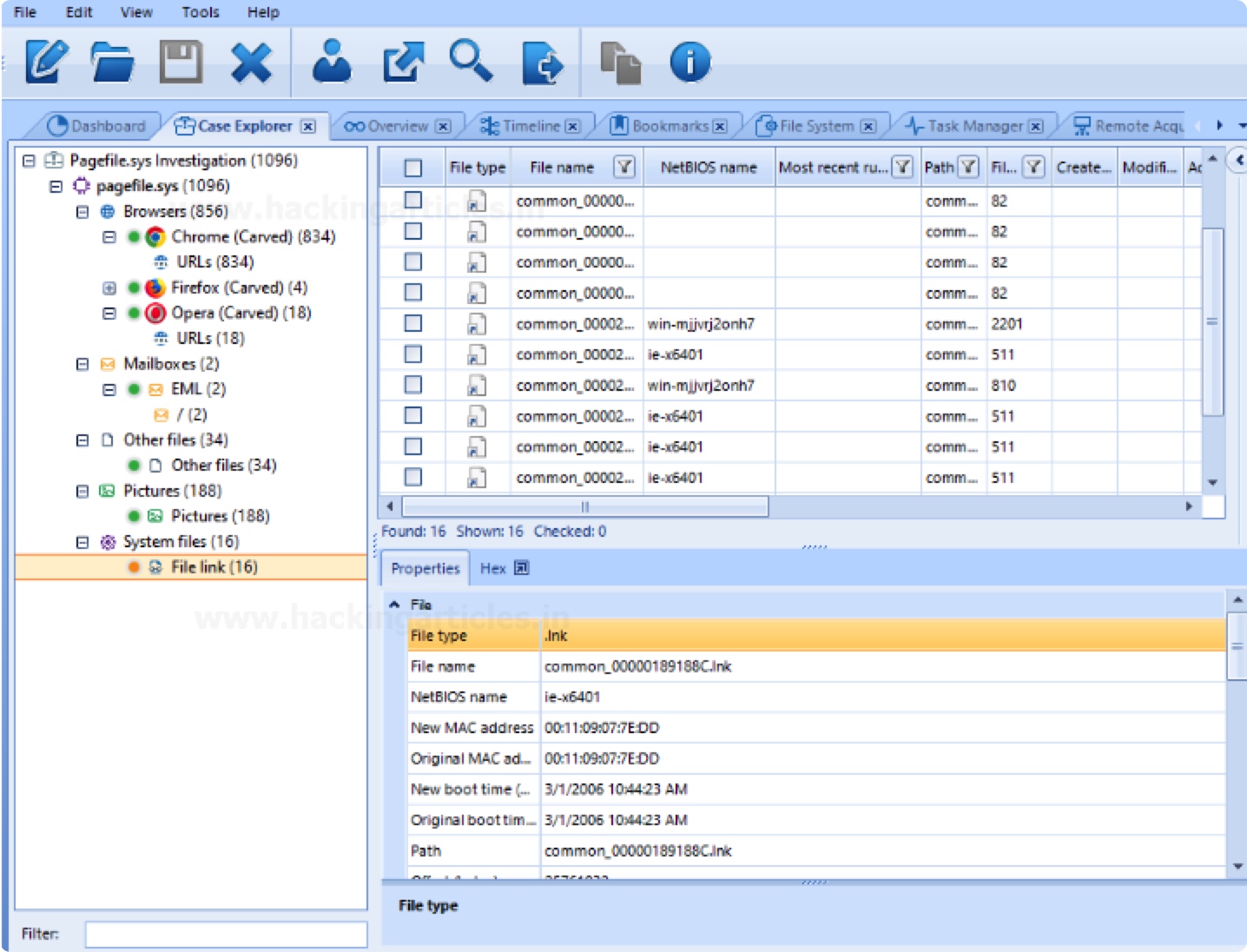
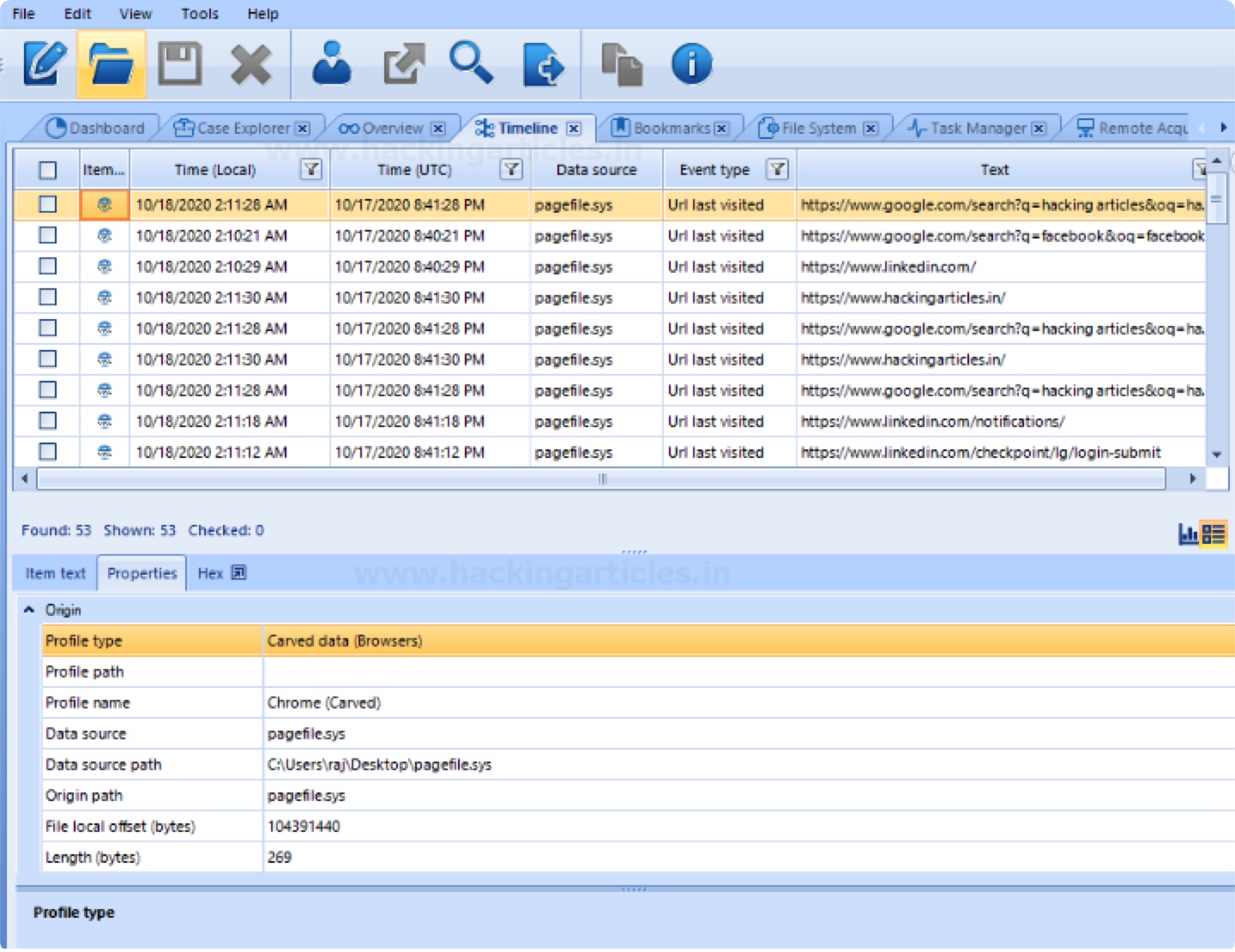


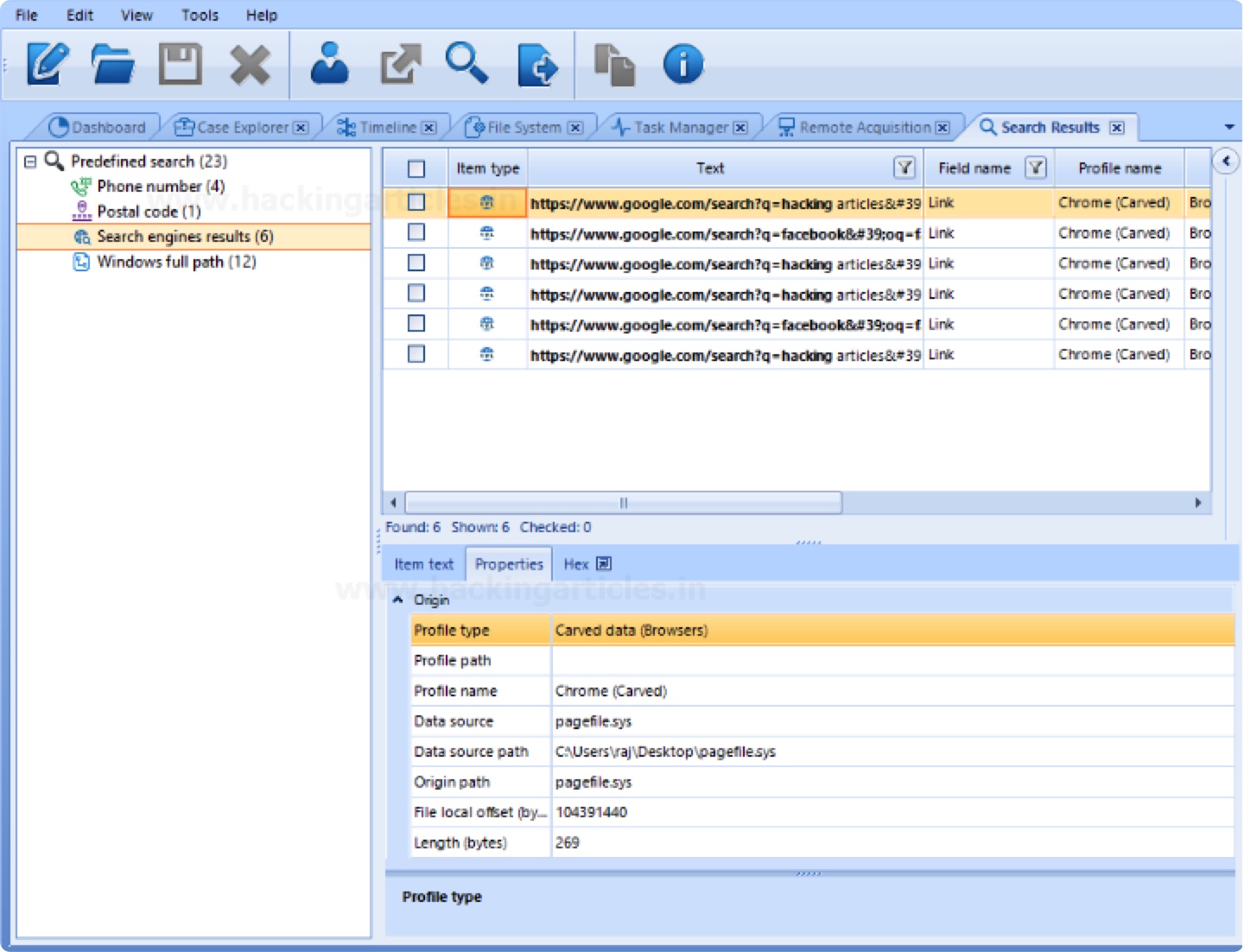
选择想要的数据类型进行搜索。这里有大量的数据类型可以扫描。点击完成按钮即可。  
  
完成了上述步骤后会显示这样一个面板。展示了正确的关于虚拟内存的统计数据信息。总数1097个文件被识别，其中包括URLs、图片和其他文件。  


在这个case explorer标签在dashboard标签旁边可以扩展和查看每个概要文件列。数据被切分为浏览器、图片、系统文件和其他文件。  


让我们展开分析Browser配置文件。让我们检查chrome切分部分的更多细节，其中之一被分为chrome历史记录包含了URLs。其中高亮的部分就是历史访问的URL地址列。



另一个浏览器配置是opera浏览器，分析opera部分的内容也是同样，其中展示了URL浏览记录。  
  
从配置文件切分的数据也包含了一些图片信息。这些图片是我访问过的网站的图片或者是其他缩略图。  
belkasoft evidence center的一个非常好的特性是，它允许你简单在图片上按右键，可以进行分析各方面，例如检查皮肤、图片中的色情信息，特定的文字或者脸。所有的这些特性都在分析的时候会起到比较有用的效果。  
  
一些系统文件也被从虚拟内存中切分，显示了NetBios名字，文件地址，文件大小等数据。  
  
时间轴标签展示了数据切分的整体情况可以通过时间和URL来进行简单的分析历史访问的网站。  


search results标签展示搜索结果概要的工具。下面的截图展示了搜索引擎返回的带有link和配置文件名的结果。  


相同的，你可以对休眠文件进行取证调查。使用FTK 在系统C:/hiberfile.sys目录下扩展hiberfil.sys（用于存储系统休眠模式下存储的信息）进行取证，并且使用Belkasoft Evidence Centre进行分析。

虚拟内存文件的分析对于浏览器鉴定有很大帮助。