

Forensic Investigation: Preserve TimeStamp

September 10, 2020 By Raj Chandel

As a Digital Forensic Investigator, you might understand, how important it is to preserve timestamps of any evidence gathered at the scene of a crime. You will be on your toes to make sure that the timestamps of the original evidence are never altered at the time of acquisition. This is important as you have to maintain the chain of custody of the evidence.

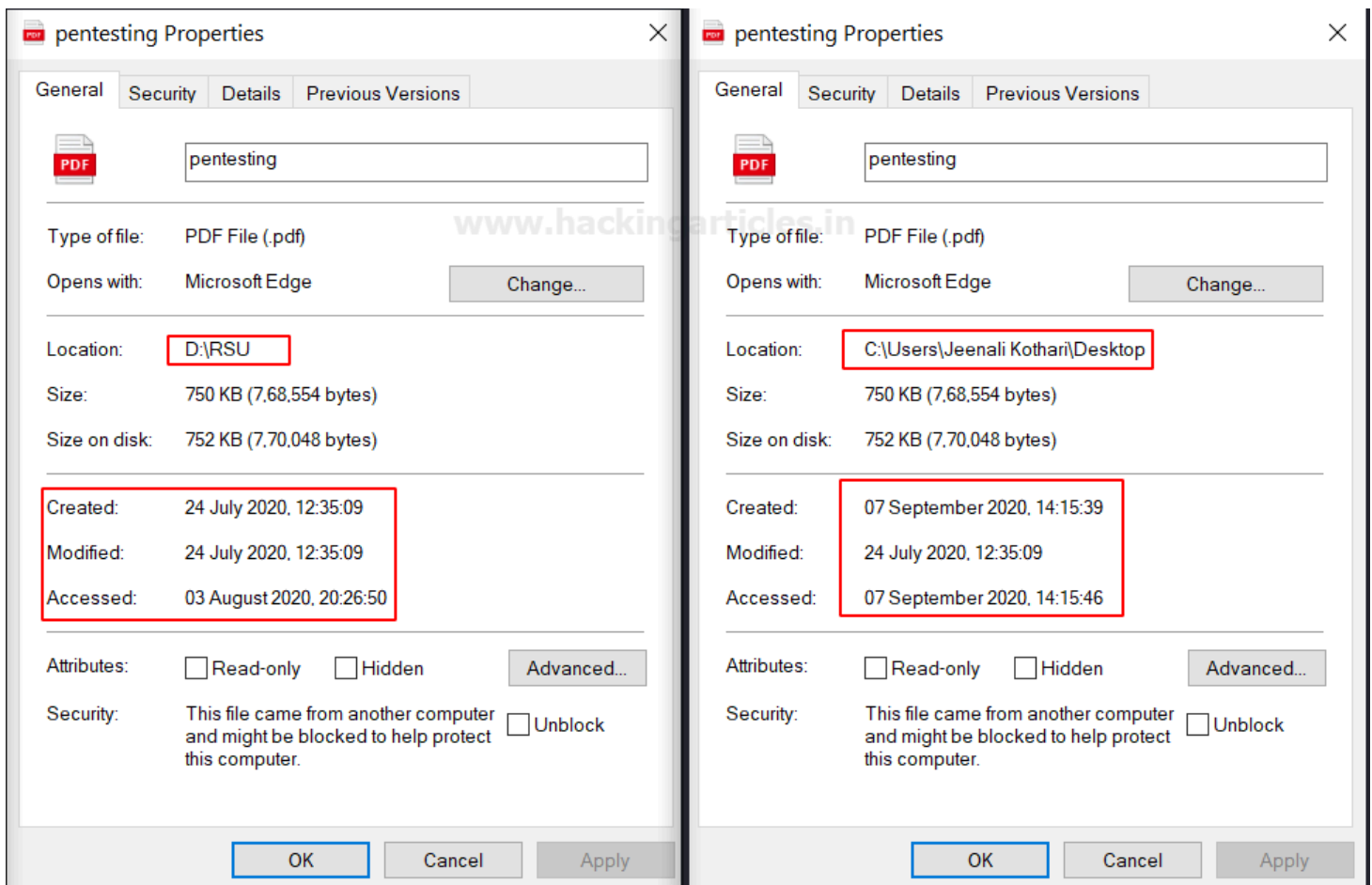
Table of Contents

- **Introduction to Timestamp**
- **Preserving Timestamp using command-prompt**
- **Preserving Timestamp using ForensicCopy**
- **Preserving Timestamp using OSForensics**
- **Preserving Timestamp using Copy Files with Dates**
- **Preserving Timestamp using SafeCopy**
- **Preserving Timestamp using TeraCopy**
- **Preserving Timestamp in Linux**

Some of the popular file systems like FAT, NTFS, and EXT store file timestamps in the following manner

TIMESTAMP	
Created Date and Time	The date and time when the file was first created.
Accessed Date and Time	The last date and time when a file was last accessed by any user.
Modified Date and Time	The last captured date and time when any modification was made to a file

Let us take a scenario where you have been investigating a case and suddenly you have the opportunity to gather evidence files or folder from a system which you had been wanting to seize for a very long time, but now you don't have your paid and expensive tools with you. If you use the traditional copy and paste method, you will be changing the timestamps of the documents



If we want to avoid these problems in our forensic investigation, we are going to learn to use a few simple forensic techniques and open-source software where you will be able to copy folder or files from one location to the other without changing the timestamps, hence preserving the timestamp.

Preserving Timestamp using command-prompt

This is one of the manual and simplest technique which does not require any fancy, expensive, or automated software to transfer files from one location to the other in a windows system with just using a command in the command prompt. The Robocopy command stands for 'Robust File Copy', which was introduced in Windows NT and has been popular ever since to copy files from one location to another robustly. You can type;

```
Robocopy D:\ E:\
```

C:\WINDOWS\system32\cmd.exe

Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Jeenali Kothari>Robocopy D:\ignite E:\

ROBOCOPY :: Robust File Copy for Windows

Started : 07 September 2020 14:36:06

Source : D:\ignite\

Dest = E:\

Files : *.*

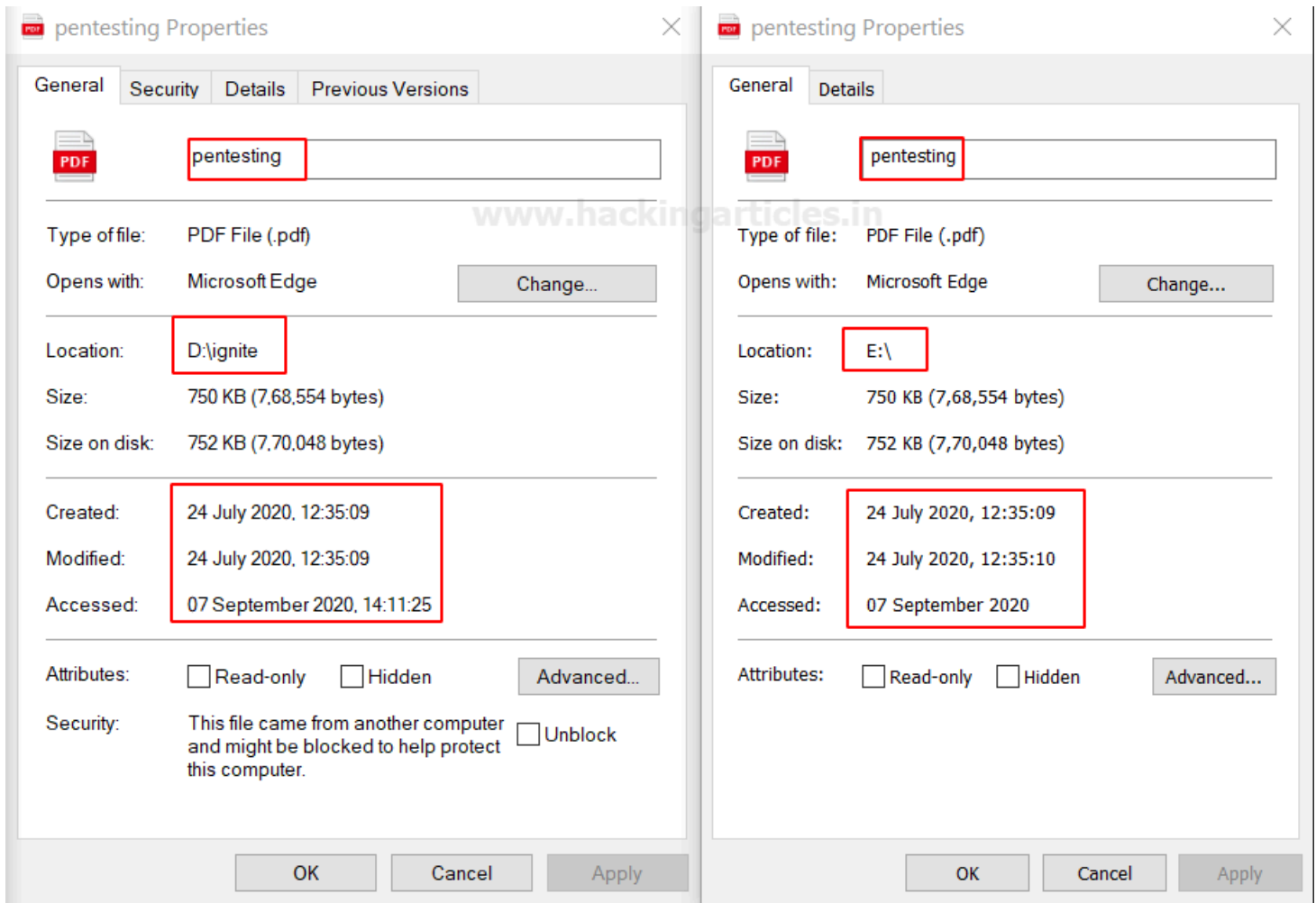
Options : *.* /DCOPY:DA /COPY:DAT /R:1000000 /W:30

	1	D:\ignite\	
*EXTRA Dir	-1	E:\System Volume Information\	
*EXTRA File	56	.dropbox.device	
*EXTRA File	162	CV.docx	
99%	New File	768554	pentesting.pdf

	Total	Copied	Skipped	Mismatch	FAILED	Extras
Dirs :	1	0	1	0	0	1
Files :	1	1	0	0	0	2
Bytes :	750.5 k	750.5 k	0	0	0	218
Times :	0:00:03	0:00:03			0:00:00	0:00:00

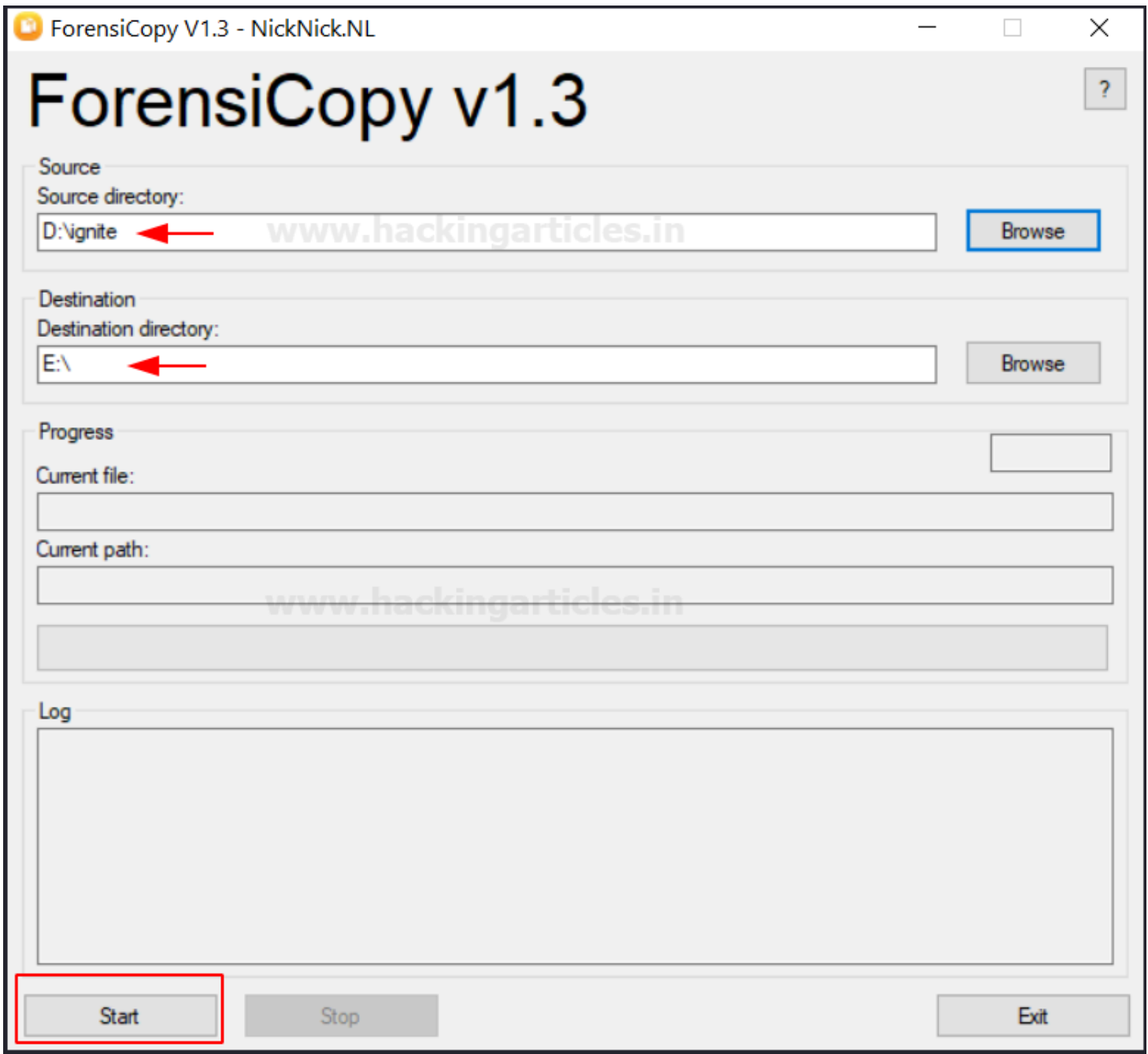
Speed : 239350 Bytes/sec.
Speed : 13.695 MegaBytes/min.
Ended : 07 September 2020 14:36:09

After the copying is completed, you can manually see that has been no difference in the date time stamp in the copy of the file.



Preserving Timestamp using ForensiCopy

ForensiCopy is an automated evidence copying software that is quite different from imaging. It can be downloaded from [here](#). This tool copies the file from one location to the other without changing the timestamps. All you have to do is, add the path of the file, the destination of the file to copy and click on start. On completion, it will generate a log file.



Once the copy is over, you can compare the source and destination properties of the files and you will see that the time was not changed.

ForensiCopy v1.3

?

Source

Source directory:

D:\HA

Browse

www.hackingarticles.in

Destination

Destination directory:

E:\ignite

Browse

Progress

3/3

Current file:

cyber security for dummies.pdf

Current path:

D:\HA\

Log

Copy started on: 07-09-2020 15:10:39
Files Copied: 3
Files Failed to Copy: 0
Folders Copied: 0
Folders Failed to Copy: 0
Total Data Copied: 31.18 MB
Copy Finished on: 07-09-2020 15:10:50
Time Elapsed: 00 Days 00 Hours 00 Minutes 11 Seconds

Export log?



Copy completed.
A log file has been generated in the ForensiCopy folder.
Would you like to export the log?

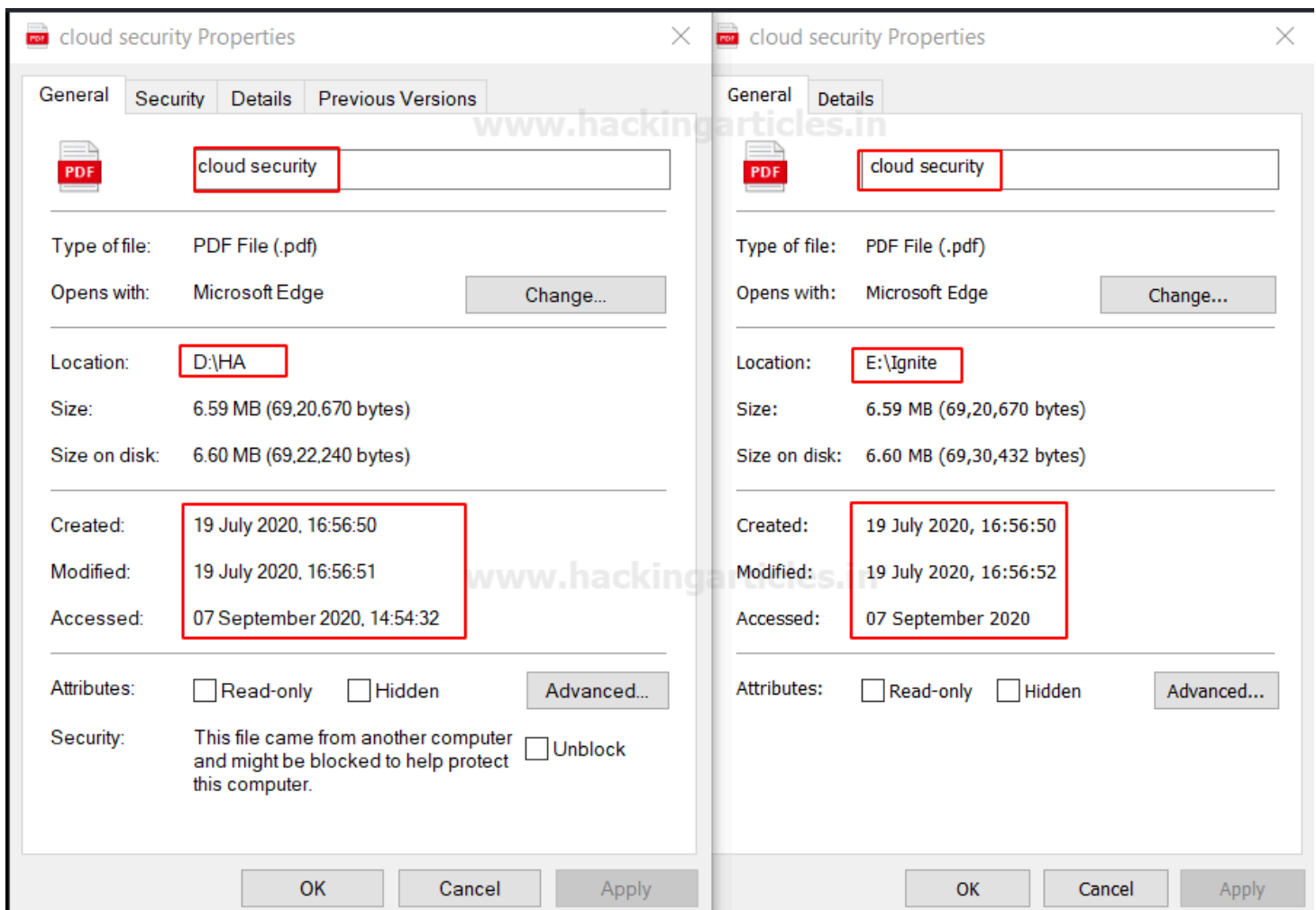
Yes

No

Start

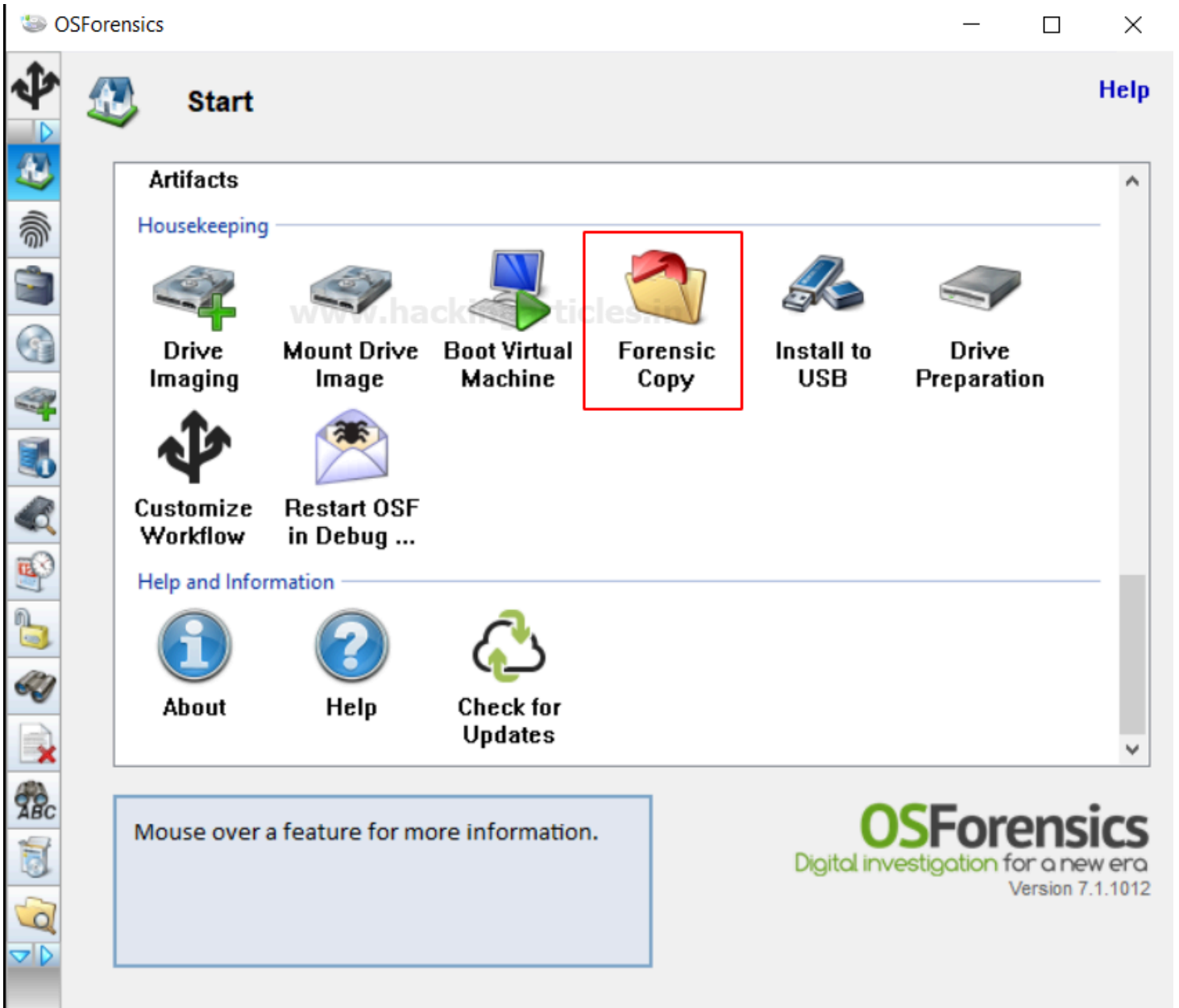
Stop

Exit

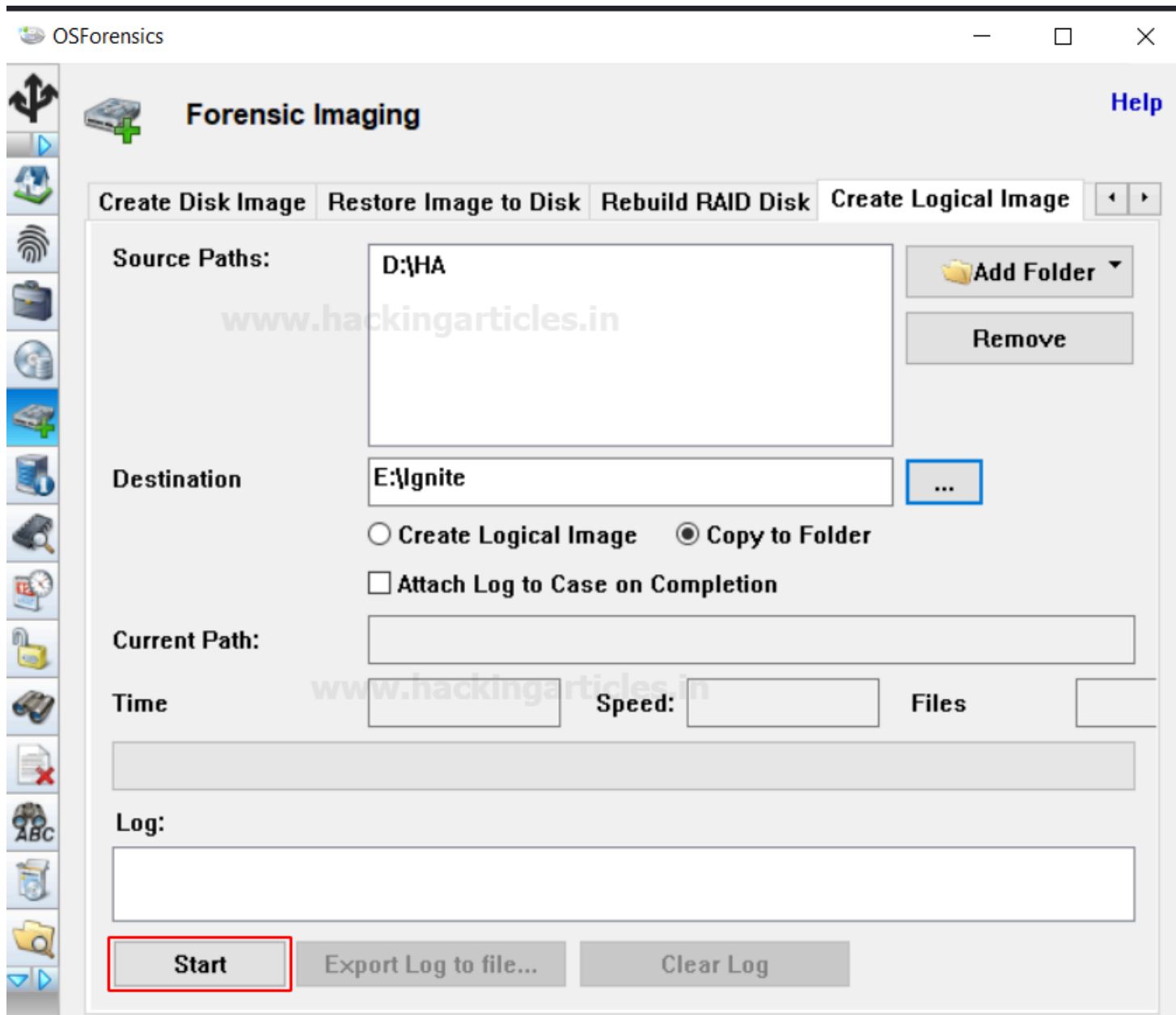


Preserving Timestamp using OSForensics

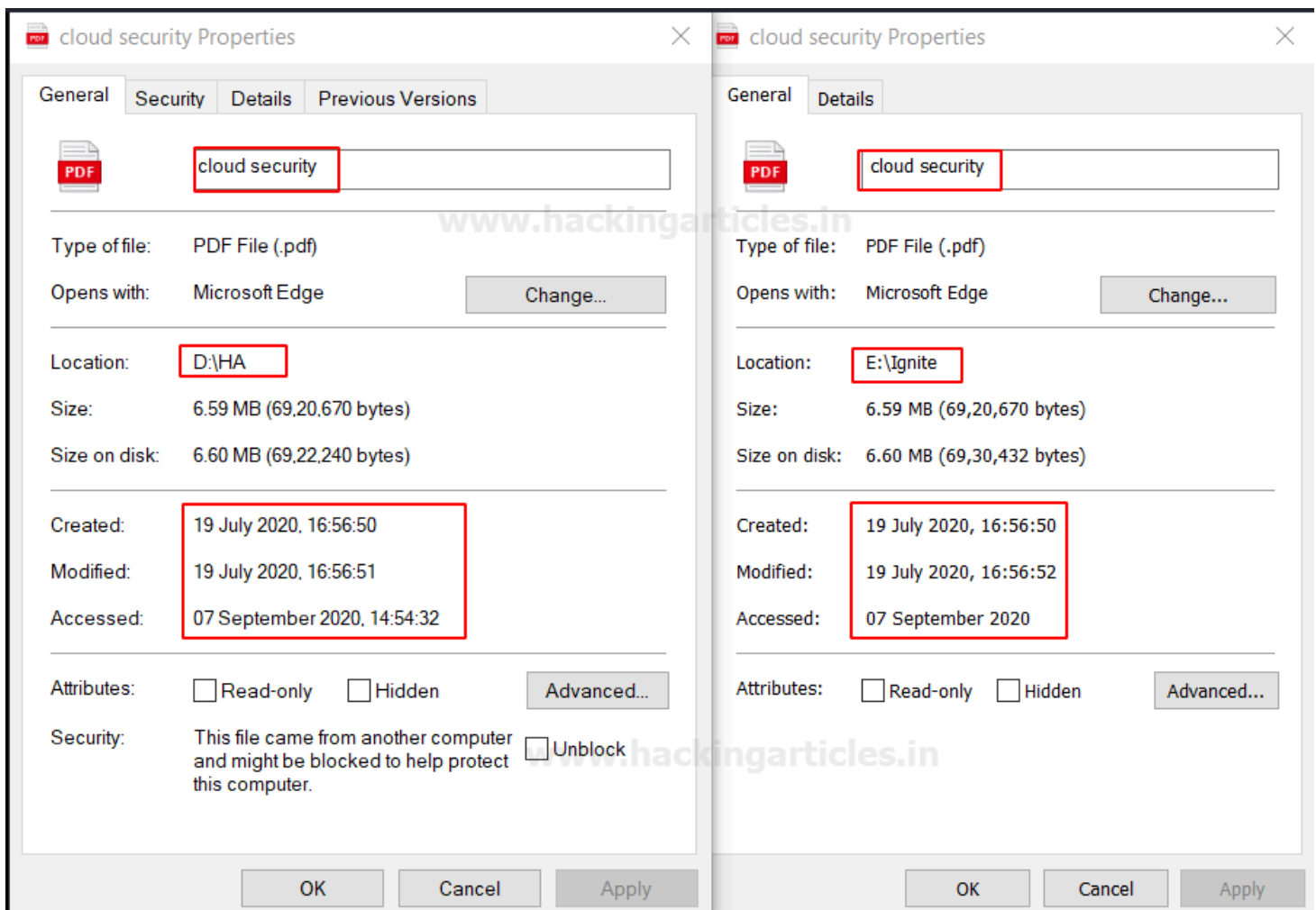
OSForensics has always been a legendary tool in forensics investigation and provides the option to make a 'Forensic Copy'. You can download it from [here](#).



Here in this software, it is called as Forensics Imaging by creating a Logical Image. In Logical Image, only a portion of a drive is copied bit by bit and keeps the timestamp of the file/folder intact. Add the source and destination path of the folder and click on start.

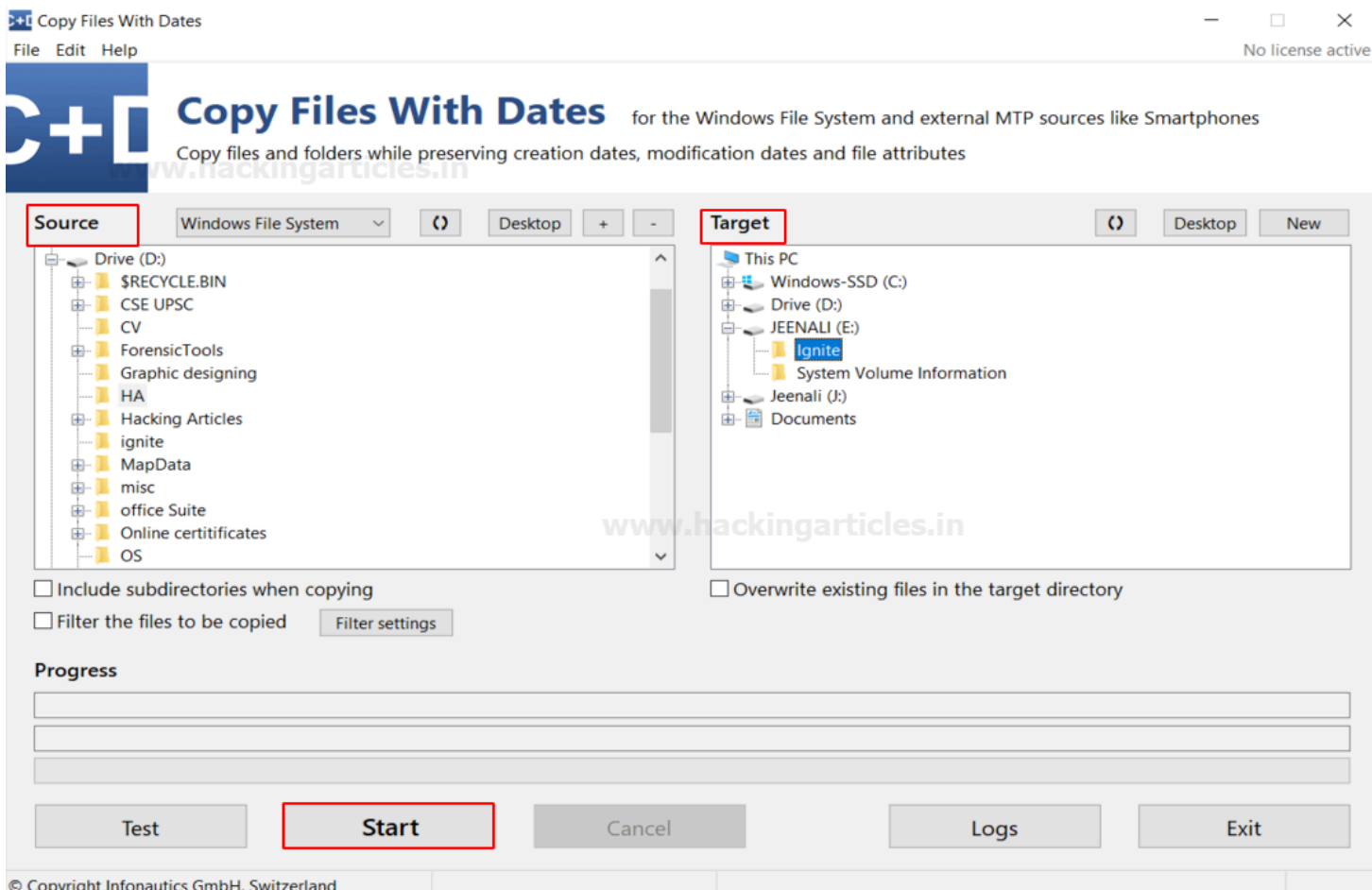


Here, you can see that the source and destination path have not changed and are intact.



Preserving Timestamp using Copy Files with Dates

This again is a crucial software when it comes to preserving the date and timestamps of any files in the Windows file system. You can download it from [here](#). All you have to do is put a source file and the destination file and click on start.



A log file will be generated which can be opened in the command prompt using

```
type name_of_log.txt
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Jeenali Kothari\AppData\Roaming\CopyFilesWithDates\Logs>type 2020-09-07_15-51-42.txt
Copy Files With Dates, Version 1.15
Actual License: Demo

2020.09.07 15:51:42

Source: D:\HA\
Target: E:\Ignite\

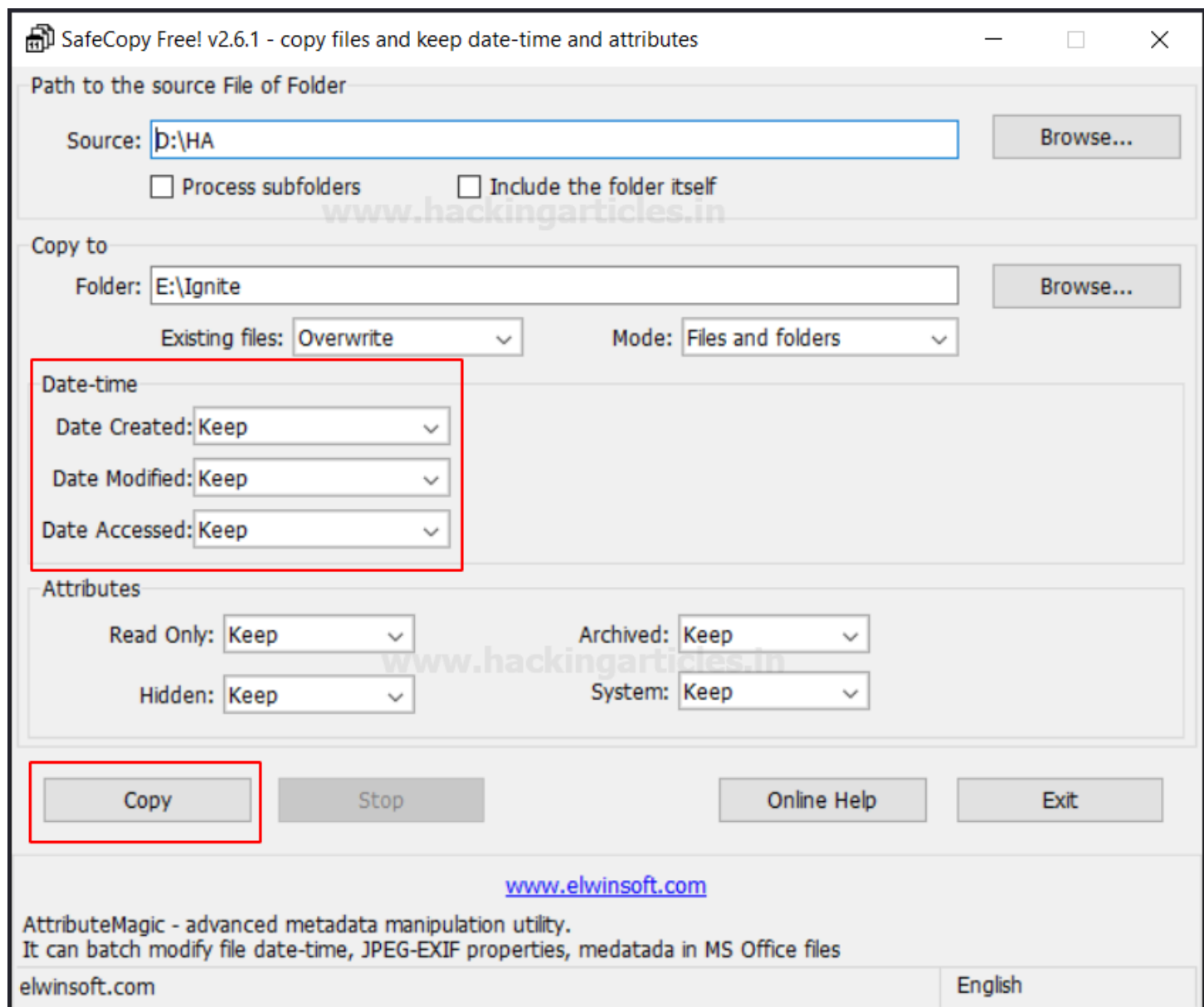
State  Creation Date  Size  Path\Filename
OK     2020.04.27 01:13:12  13820119  D:\HA\blue team cheat sheet.pdf
OK     2020.07.19 16:56:50  6920670  D:\HA\cloud security.pdf
OK     2020.04.26 12:05:10  11952948  D:\HA\cyber security for dummies.pdf
OK     2020.07.19 18:12:18  2919585  D:\HA\cyber threat insights.pdf

Copied: 4 Files, 35613322 Bytes

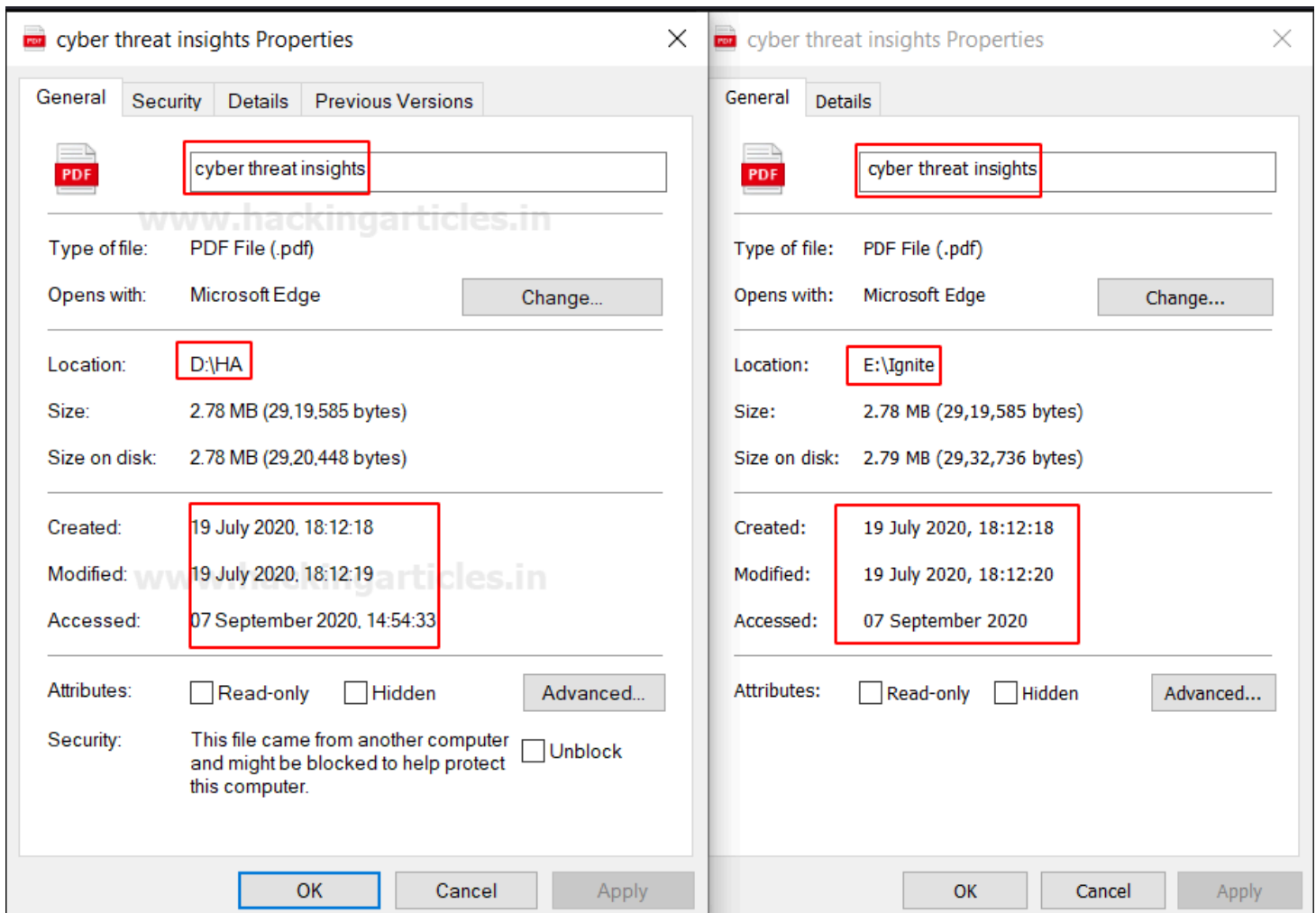
2020.09.07 15:51:52
```

Preserving Timestamp using SafeCopy

It is a software which can be used to perform forensics as well as anti-forensics. You can download it from [here](#). Add the source and the destination path and keep the same date and time of the file to preserve it and then click on copy.

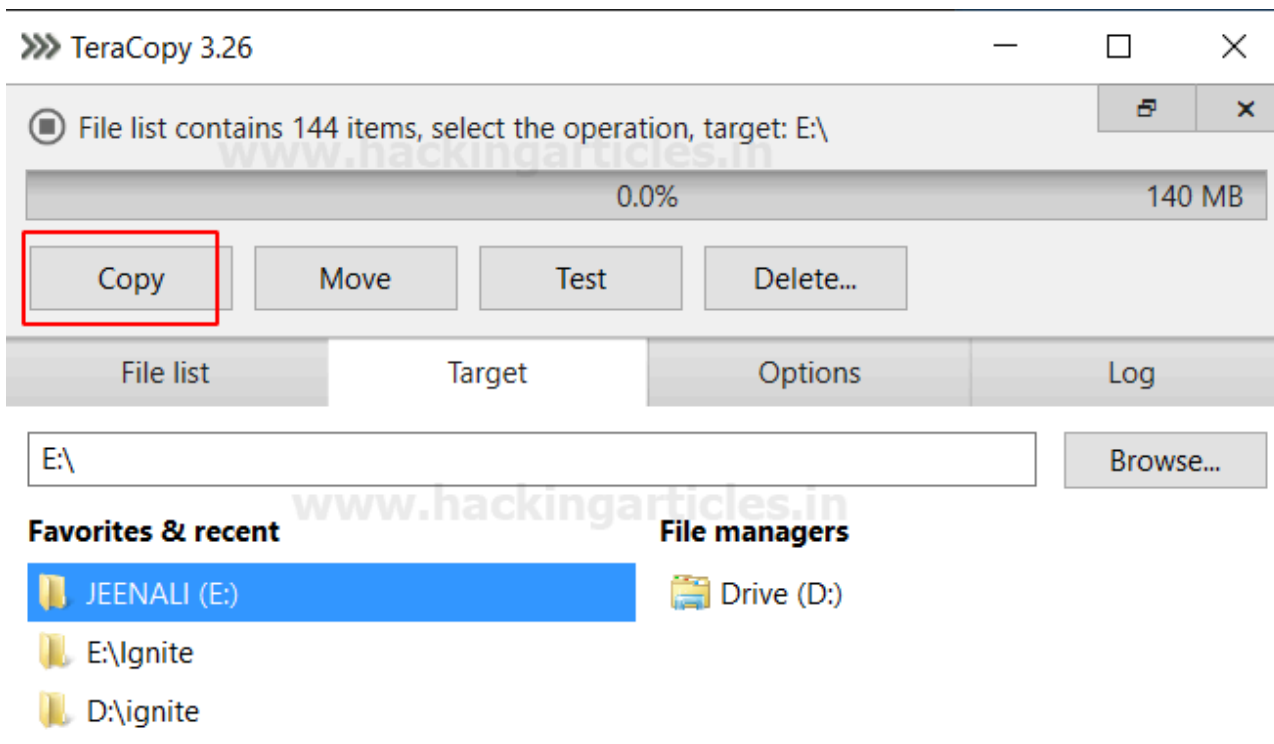


You will see below, that the timestamps for these files that have been copied to a new destination are intact.



Preserving Timestamp using TeraCopy

It is a quite simple tool and barely any consumes very little time to copy the files to the destination without changing the date and time of the original document. You can download it from [here](#).



Preserving Timestamp in Linux


So here you can switch on your Linux machines and open your terminal as root. Go to the directory of the source of the file to be copied and type

```
ls -al
```

```
root@Jeenali:/home/jeenali/Desktop/autopsy# ls -al
total 952
drwxr-xr-x 2 jeenali jeenali 4096 Sep  7 15:32 .
drwxr-xr-x 6 jeenali jeenali 4096 Sep  7 15:31 ..
-rw-r--r-- 1 jeenali jeenali 134132 Aug 13 15:18 18.png
-rw-r--r-- 1 jeenali jeenali 61087 Aug 13 15:50 19.png
-rw-r--r-- 1 jeenali jeenali 101875 Aug 13 15:34 20.png
-rw-r--r-- 1 jeenali jeenali 54900 Aug 13 15:47 21.png
-rw-r--r-- 1 jeenali jeenali 84325 Aug 13 15:51 22.png
-rw-r--r-- 1 jeenali jeenali 72645 Aug 13 15:53 23.png
-rw-r--r-- 1 jeenali jeenali 42535 Aug 13 15:54 24.png
-rw-r--r-- 1 jeenali jeenali 37133 Aug 13 15:55 25.png
-rw-r--r-- 1 jeenali jeenali 82880 Aug 13 23:34 26.png
-rw-r--r-- 1 jeenali jeenali 109099 Aug 13 23:37 27.png
-rw-r--r-- 1 jeenali jeenali 92161 Aug 13 23:40 28.png
-rw-r--r-- 1 jeenali jeenali 71381 Aug 13 23:42 29.png
root@Jeenali:/home/jeenali/Desktop/autopsy#
```


To copy the file without changing time stamp, use command;

```
cp -p 18.png /home/jeenali/Desktop/ignite
```

```
root@Jeenali:/home/jeenali/Desktop/autopsy# cp -p 18.png /home/jeenali/Desktop/Ignite   
root@Jeenali:/home/jeenali/Desktop/autopsy#
```

You can see that it has been copied to a new destination without the timestamp changing, to see the file information at the new path, type;

```
ls -al
```

```
root@Jeenali:/home/jeenali/Desktop/Ignite# ls -al   
total 140  
drwxr-xr-x 2 jeenali jeenali 4096 Sep  7 15:35 .  
drwxr-xr-x 7 jeenali jeenali 4096 Sep  7 15:34 ..  
-rw-r--r-- 1 jeenali jeenali 134132 Aug 13 15:18 18.png  
root@Jeenali:/home/jeenali/Desktop/Ignite#
```

Conclusion: Hence, here in this article you have learnt about various methods and tools to copy files from one location to the other without changing the timestamp.