Autopsy

Task 2 Workflow Overview and Case Analysis

What is the file extension of the Autopsy files?

.aut

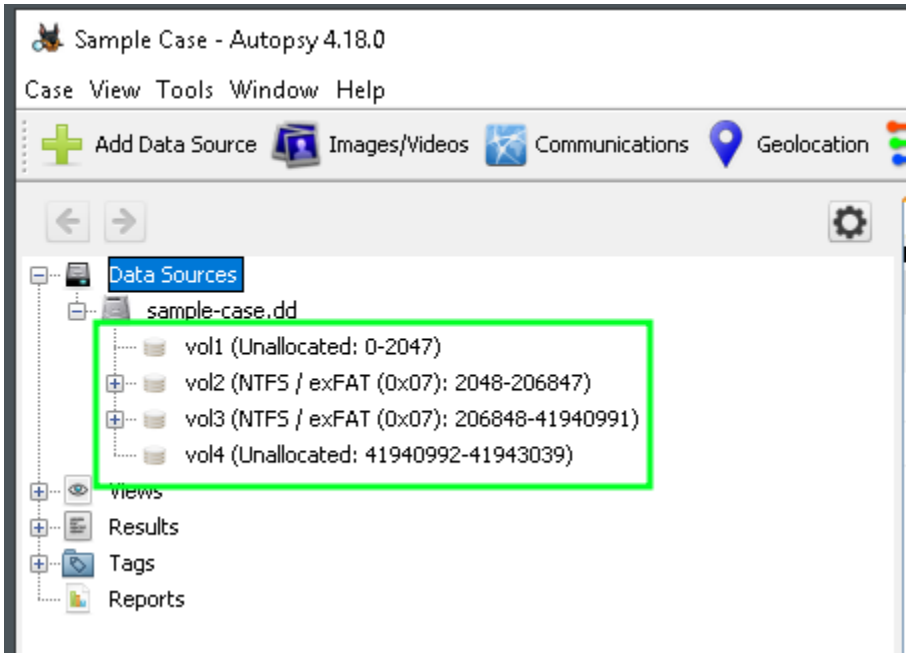
Task 3 Data Sources

What is the disk image name of the "e01" format?

Encase

Task 5 The User Interface I

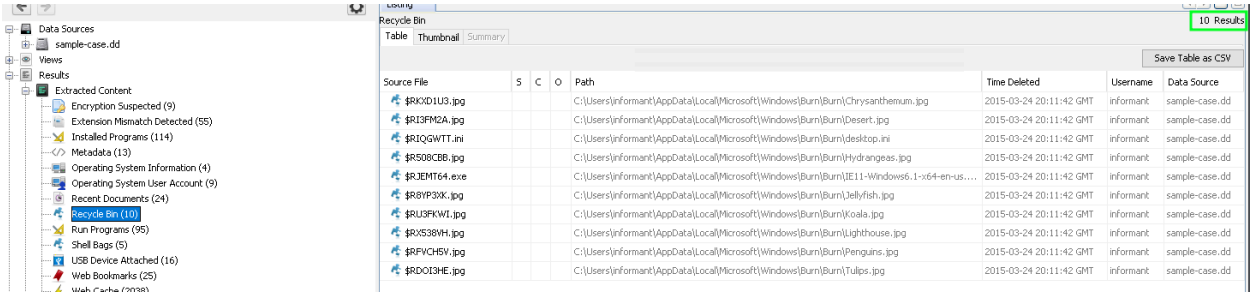
Expand the "Data Sources" option; what is the number of available sources?



4

What is the number of the detected "Removed" files?

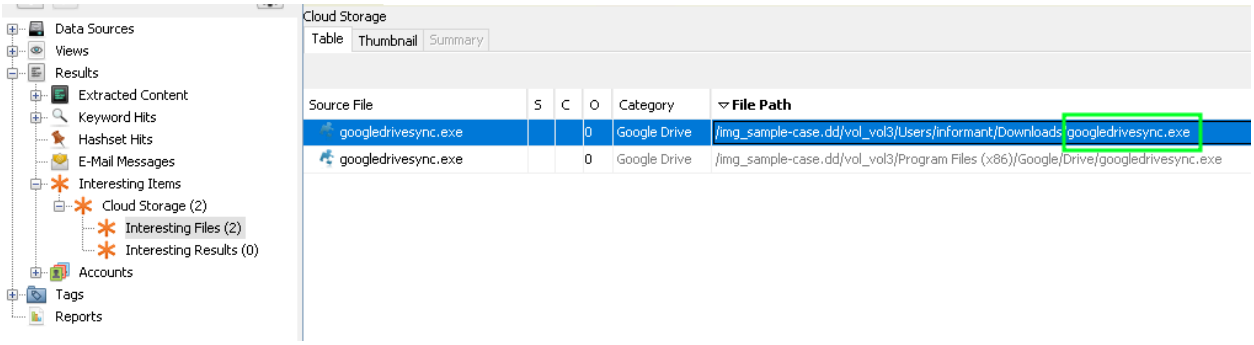
Available in **Results > Extracted Company > Recycle Bin**



10

What is the filename found under the "Interesting Files" section?

It is available at Result -> Interesting Items -> cloud storage -> Interesting files

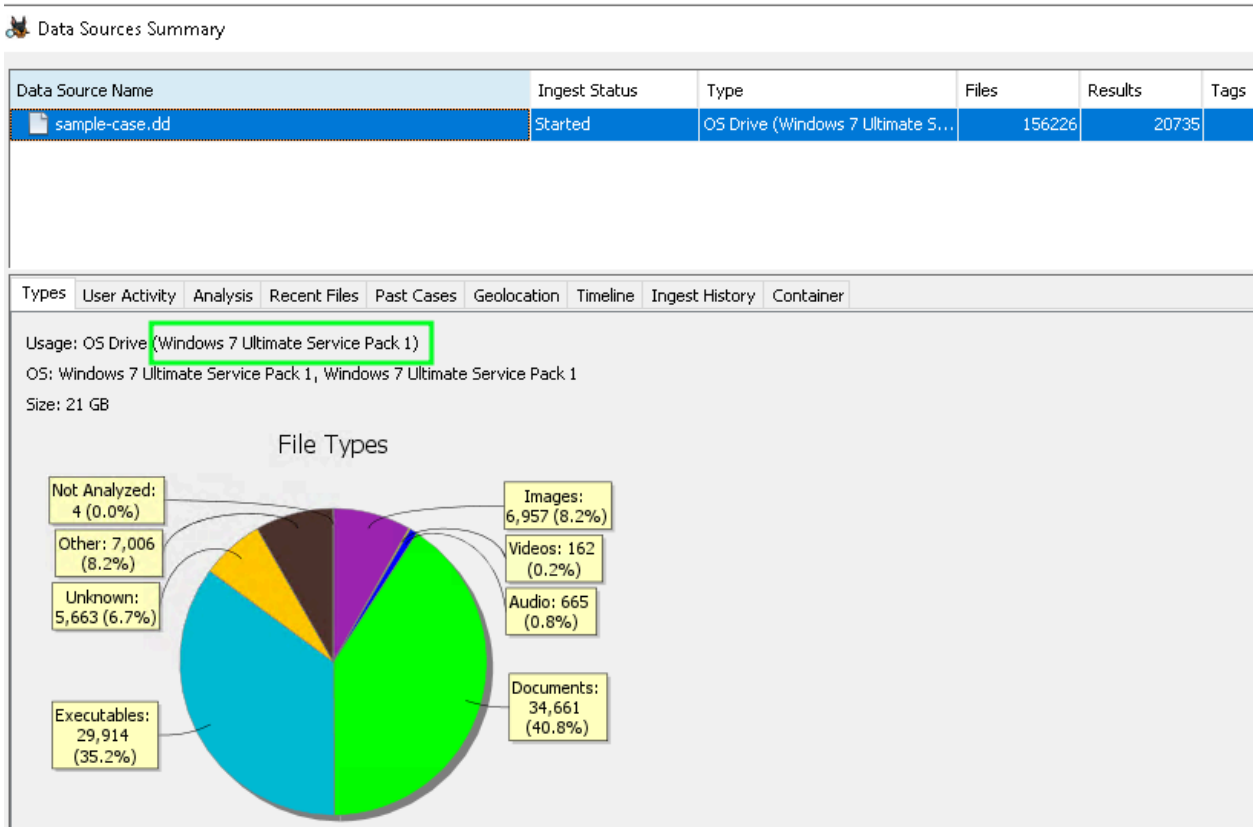


googledrivesync.exe

Task 6 The User Interface II

What is the full name of the operating system version?

Right click on the data sources -> view summary



Windows 7 Ultimate Service Pack 1

What percentage of the drive are documents? Include the % in your answer.

Observe the pie chart 40.8%

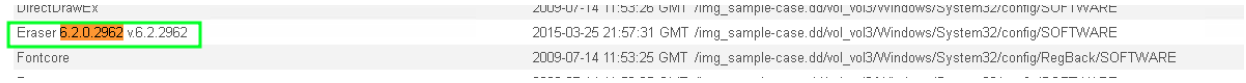
Generate an HTML report as shown in the task and view the "Case Summary" section. What is the job number of the "Interesting Files Identifier" module?

Generat the report , open the report -> Case Summary , scroll to the bottom you will find interesting file finder

Task 7 Data Analysis

What is the name of an Installed Program with the version number of 6.2.0.2962?

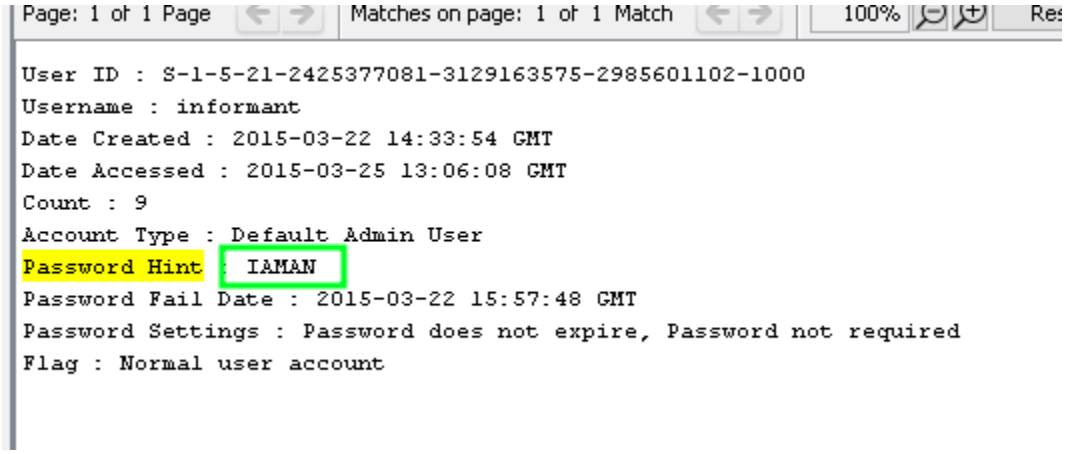
I am using the previously generated report , click on the installed programs section in the left side then search for the version 6.2.0.2962



Eraser

A user has a Password Hint. What is the value?

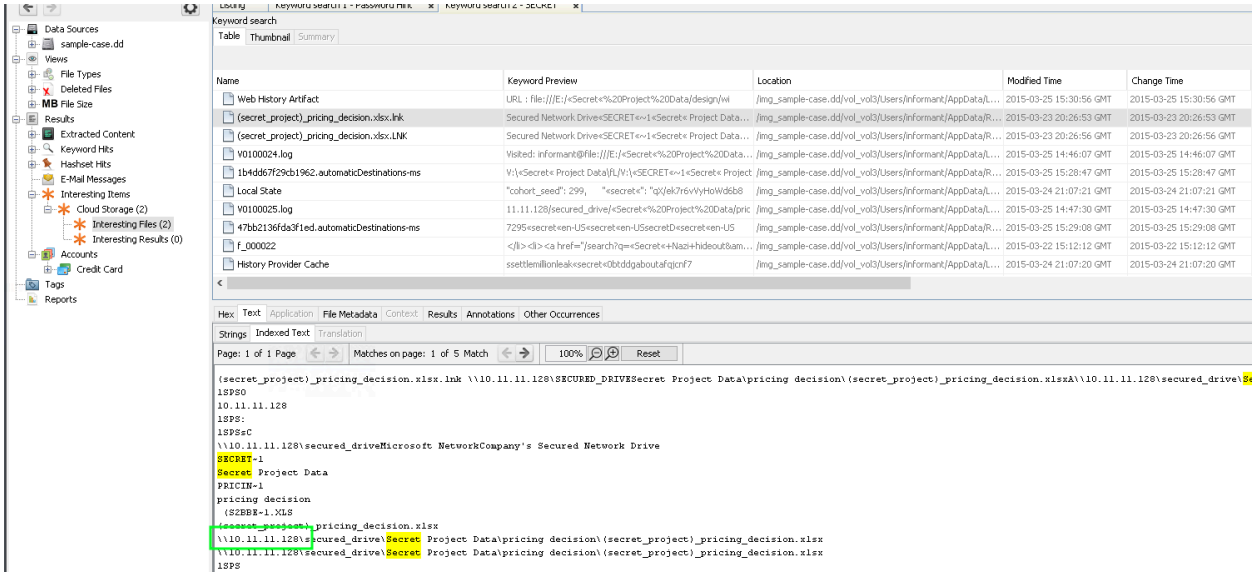
Search for the Password Hint in the keyword search section



IAMAN

Numerous SECRET files were accessed from a network drive. What was the IP address?

Search for the secret



10.11.11.128

What web search term has the most entries?

Refer to the report -> web search (at the bottom , left panel) , observe the searches

information leakage cases

What was the web search conducted on 3/25/2015 21:46:44?

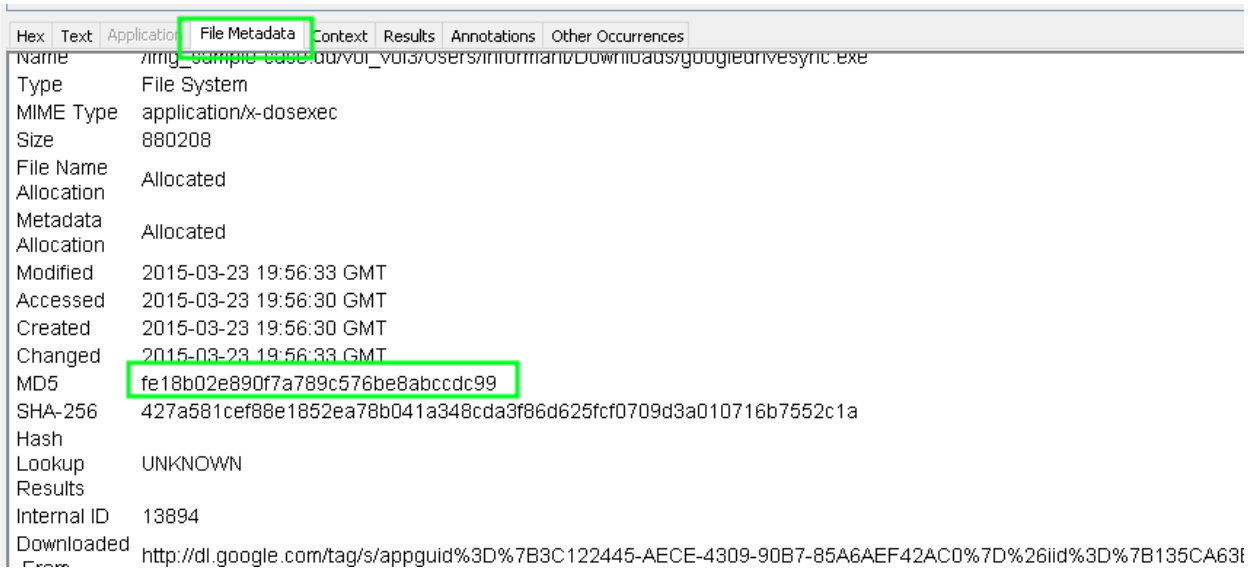
Search for the timing in the report (web search)

anti-forensic tools

What MD5 hash value of the binary is listed as an Interesting File?

In the autopsy Result -> Interesting Items -> cloud storage -> Interesting files

Click on the file -> metadata



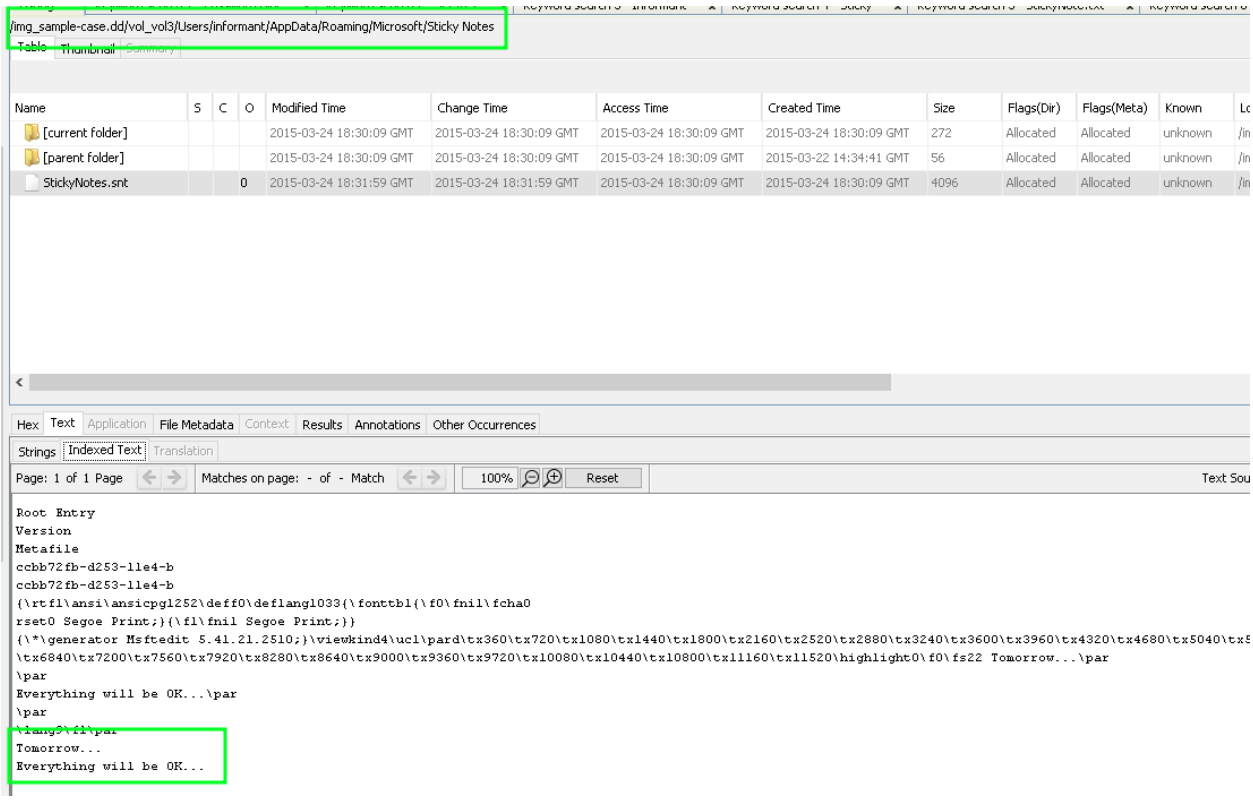
fe18b02e890f7a789c576be8abccdc99

What self-assuring message did the 'Informant' write for himself on a Sticky Note? (no spaces)

I find the answer in a file

> /img_sample-case.dd/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Sticky Notes/StickyNotes.snt

while searching



Tomorrow...Everything will be OK…

Task 8 Visualisation Tools

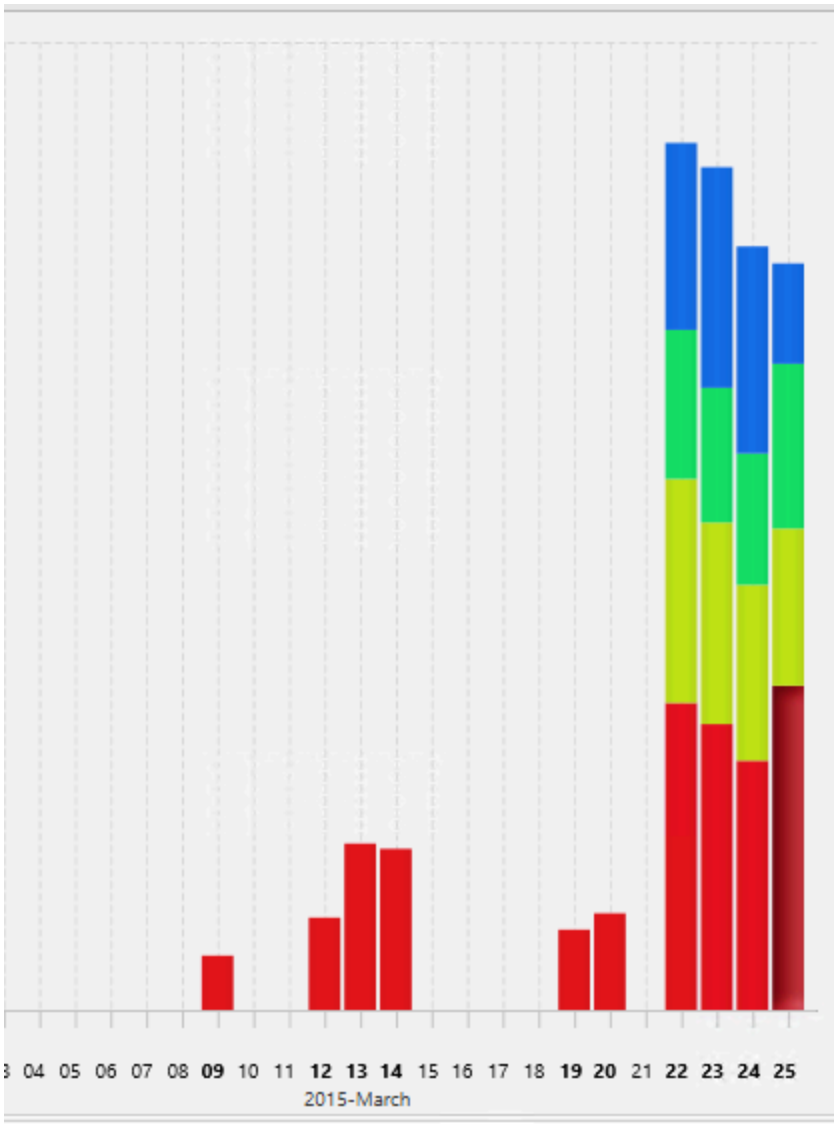
Using the Timeline, how many results were there on 2015-01-12?

Change the time to 2015-01-12 , and time from 12 AM to 11:30 PM

46

The majority of file events occurred on what date? (MONTH DD, YYYY)

Observe the graph clearly



March 25 , 2015