

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# TryHackMe Autopsy Write-Up



Toumo · [Follow](#)

8 min read · Aug 7, 2023



Listen



Share

... More



Image from tryhackme.com

We just finished Linux Forensics, utilizing the terminal to view artifacts. We're going to be using an application called Autopsy to continue our Digital Forensics training. I wanted to utilize it more during Windows Forensics room but looks like we will have a chance now since it's all about Autopsy!

## Task 2 Workflow Overview and Case Analysis

I will be RDPing into THM's machine. Directions can be found [here](#).

1: What is the file extension of the Autopsy files?

I followed the instructions and imported Sample Case.aut. The reading also states what file extension Autopsy has.

Answer: .aut

## Task 3 Data Sources

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

I used EnCase in school so I remember this. The reading does specify which application uses .e01 format though!

Answer: EnCase

## Task 5 The User Interface I

1: Expand the “Data Sources” option; what is the number of available sources?

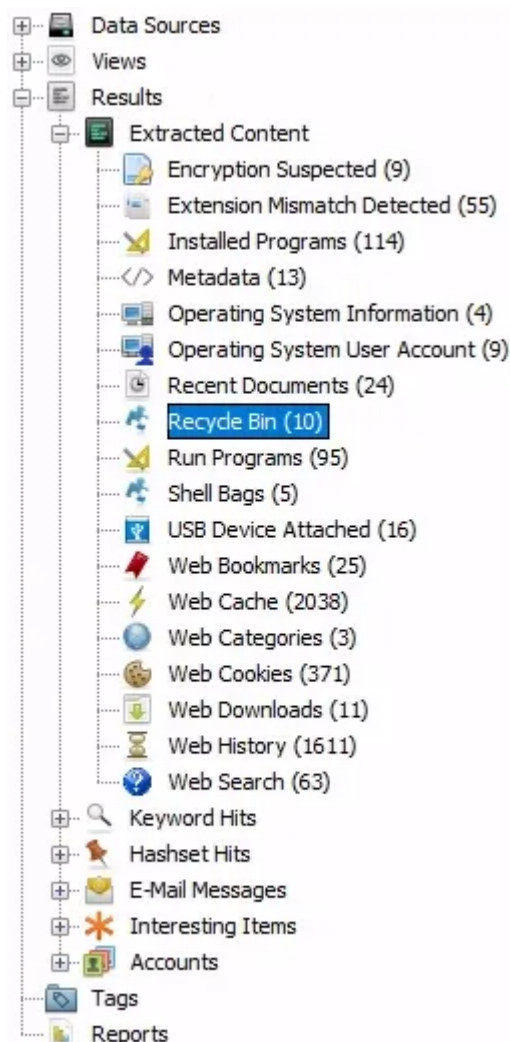
On the left side, click on “Data Sources” to expand the menu, then expand the “sample-case.dd” too and count the number of volumes.



Answer: 4

2: What is the number of the detected “Removed” files?

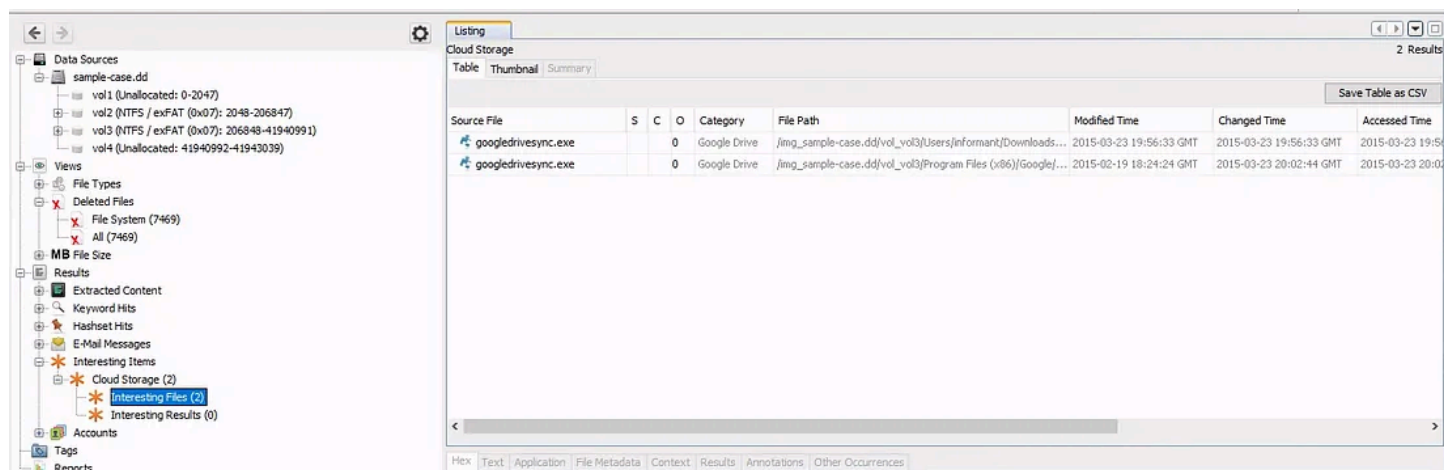
I struggled with this one. I didn't know there was a “Recycle Bin” section under “Results.” I was too focused on the one that was located in Data Sources -> sample-case.dd -> vol3 -> \$Recycle.Bin. I even used the hint for this and struggled real hard. I had to use external help. I used [this](#) to understand where the answer was found.



Answer: 10

3: What is the filename found under the “Interesting Files” section?

On the left hand side, expand “Interesting Items” until you can get to the files. Click on the files and on the right side, you can see two .exe files. That is the answer.

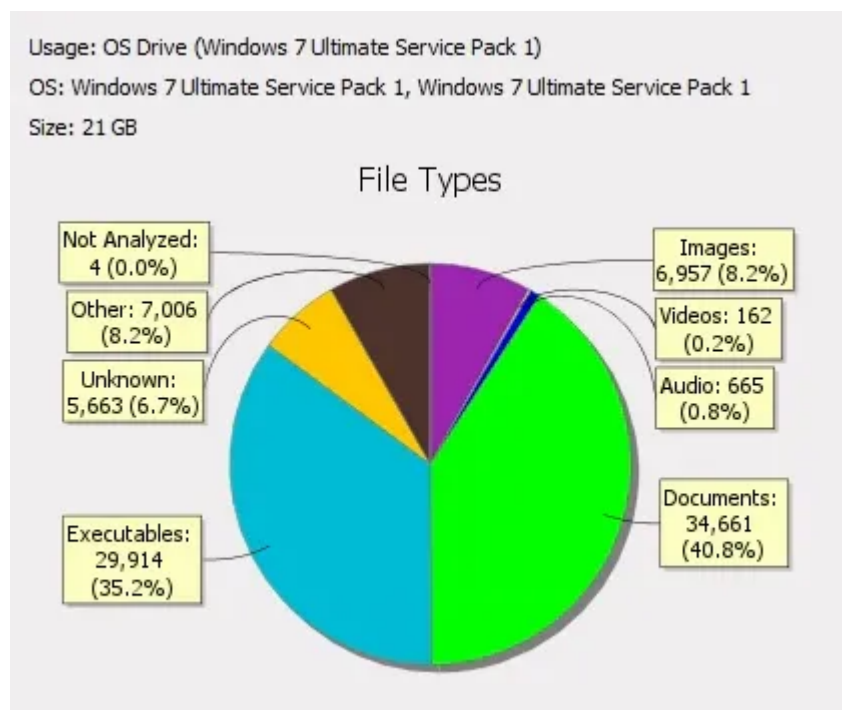


Answer: googledrivesync.exe

## Task 6 The User Interface II

1: What is the full name of the operating system version?

Using what I just read, I right clicked “sample-case.dd” and then selected “View Summary Information” to get an overview of what I’m working with. We can see the OS in this screen.



Answer: Windows 7 Ultimate Service Pack 1

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

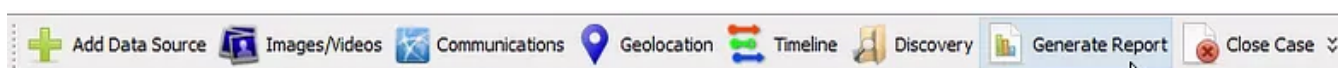
The answer can be found in the same screen as the OS version.

Answer: 40.8%

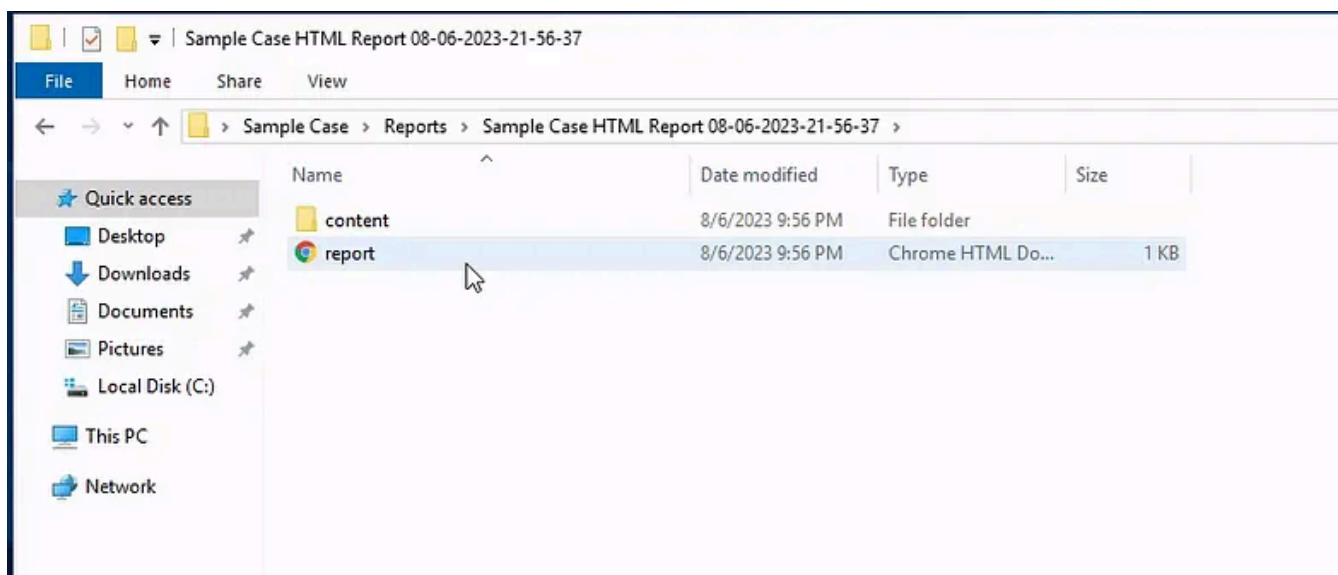
3: Generate an HTML report as shown in the task and view the “Case Summary” section.

What is the job number of the “Interesting Files Identifier” module?

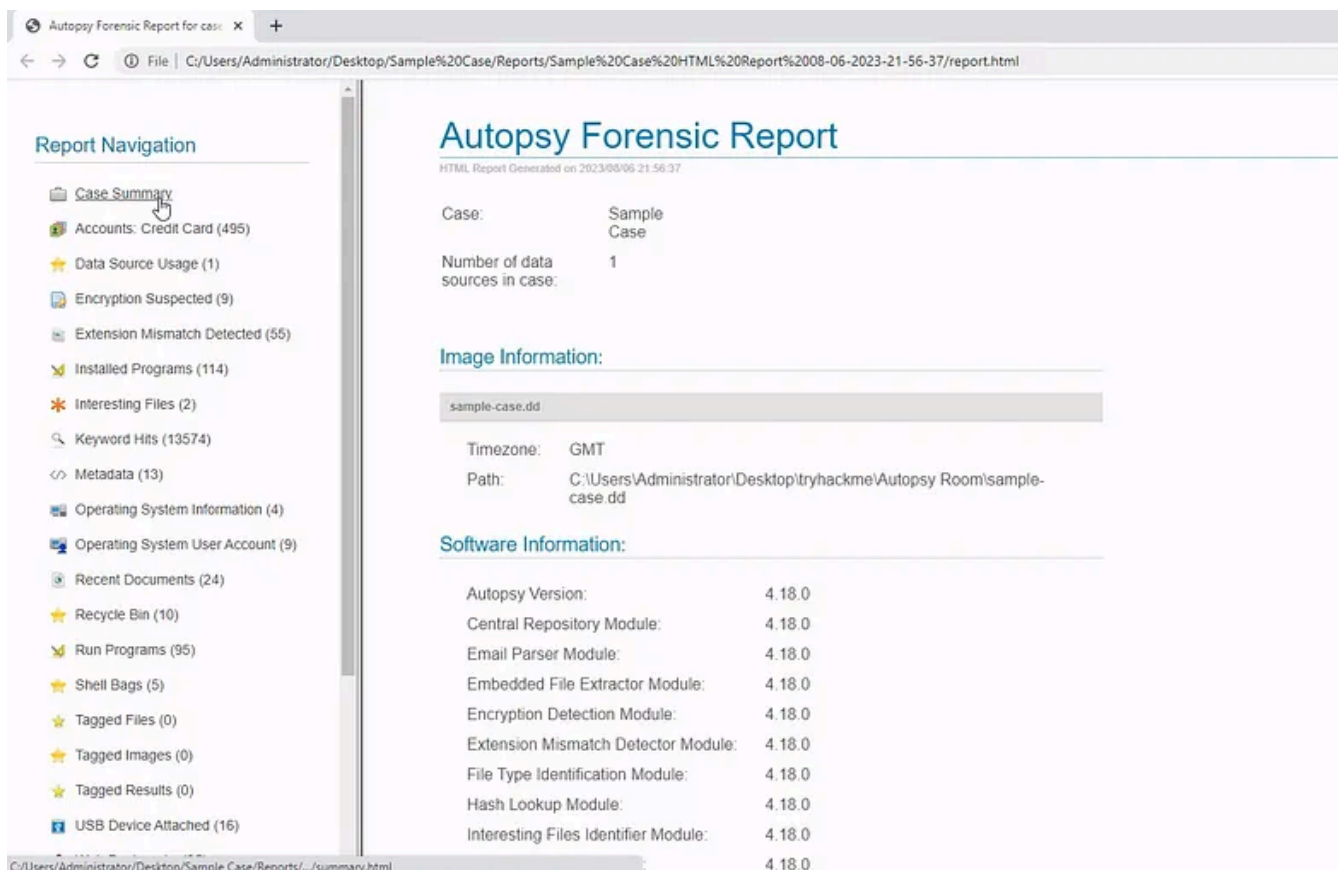
At the top, click on “Generate Report”, and select “HTLM” option. Then select “Next” twice and then click on “Finish.”



To open the report we generated, head back over to Sample Case -> Reports -> Sample Case HTML Report -> report. That should be the default location it exports to.



Once you open it, the report should look like this. Scroll down to get the job number related to Interesting Files. If your screen doesn't look like mine, just click on Case Summary at the top left and then scroll down.



## Job 10:

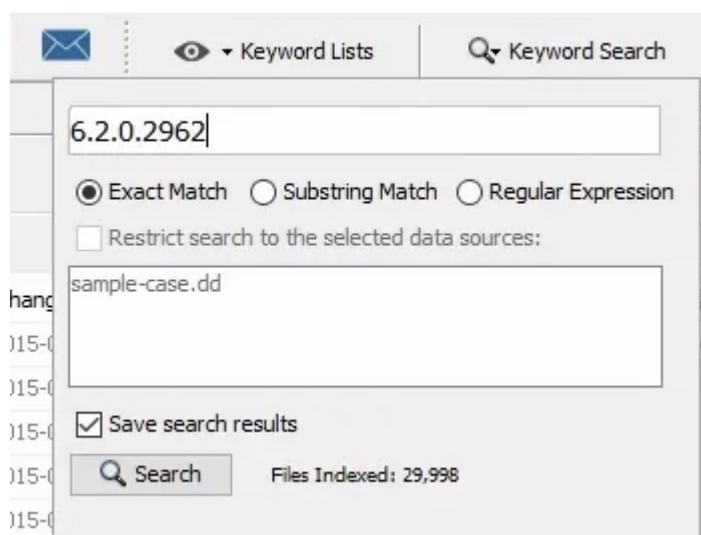
Data Source: sample-case.dd  
Status: COMPLETED  
Enabled Modules: Interesting Files Identifier

Answer: 10

## Task 7 Data Analysis

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

The first thing I did was searching for the version number by utilizing the “Keyword Search” on the top right.



Out of all the results, I saw what I felt like was the answer. The keywords said ProductVersion.

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
Eraser.exe	ProductVersion=6.2.0.2962<Assembly Version=6.2.0.2962...	/img_sample-case.dd/vol_vol3/Program Files/Eraser/Eraser...	2015-01-12 22:56:36 GMT	2015-03-25 14:57:31 GMT	2015-03-25 14:57:31 GMT

Answer: Eraser.

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

This time, I searched for Password hint to see if I can get any results. I got lucky and it did!



The screenshot shows the Autopsy Keyword Search interface. The search term is "Password Hint". The results table lists several files with their keyword previews and locations. The "Operating System User Account Artifact" file has a preview showing "Default Admin User Password Hint : IAMANPassword Fail".

Name	Keyword Preview	Location	Modified
Help_MKWD_BestBet.H1W	computerpassword expire password hint password policy...	/img_sample-case.dd/vol_vol3/ProgramData/Microsoft/Assi...	2010-11-
Operating System User Account Artifact	Default Admin User Password Hint : IAMANPassword Fail	/img_sample-case.dd/vol_vol3/Windows/System32/config/...	2015-03-
Help_MTOC_help.H1H	Create or change a password hint Internet and network	/img_sample-case.dd/vol_vol3/ProgramData/Microsoft/Assi...	2010-11-
RegRipper /img_sample-case.dd/vol_vol3/Windows/System32/conf Name	: Password Hint : IAMANLast Login	RegRipper /img_sample-case.dd/vol_vol3/Windows/System...	

Answer: IAMAN

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

I decided to search for "SECRET" first since it seems weird how it was capitalized. I ended up with some results with "Secured Network Drive" in their keyword.

The screenshot shows the Autopsy Keyword Search interface with the search term "SECRET". The results table lists several files with their keyword previews and locations. The "(secret\_project)\_pricing\_decision.xlsx.lnk" file has a preview showing "Secured Network Drive SECRET ~1 Secret Project Data...".

Name	Keyword Preview	Location	Modified
Web History Artifact	URL : file:///E:/Secret/ProjectData/design/wi	/img_sample-case.dd/vol_vol3/Users/Informant/AppData/L...	2015-03-
(secret_project)_pricing_decision.xlsx.lnk	Secured Network Drive SECRET ~1 Secret Project Data...	/img_sample-case.dd/vol_vol3/Users/Informant/AppData/R...	2015-03-
(secret_project)_pricing_decision.xlsx.LNK	Secured Network Drive SECRET ~1 Secret Project Data...	/img_sample-case.dd/vol_vol3/Users/Informant/AppData/R...	2015-03-
V0100024.log	Visited: informant@file:///E:/Secret/ProjectData...	/img_sample-case.dd/vol_vol3/Users/Informant/AppData/L...	2015-03-
1b-4dd67f29cb1962.automaticDestinations-ms	V:\Secret Project Data\N:\Secret ~1 Secret Project	/img_sample-case.dd/vol_vol3/Users/Informant/AppData/R...	2015-03-

I then clicked on the result and then looked at the bottom to see if there was anything I can get from that. It turns out there is an IP Address. I believe it was on our network because of "\\10.11.11.128\Secured\_DRIVESecret...." which made me think it was mapped to the network.

The screenshot shows the Autopsy Strings view for the selected file. The search term is "SECRET". The results show the string "\\10.11.11.128\Secured\_DRIVESecret...." in the file path.

Strings Indexed Text Translation

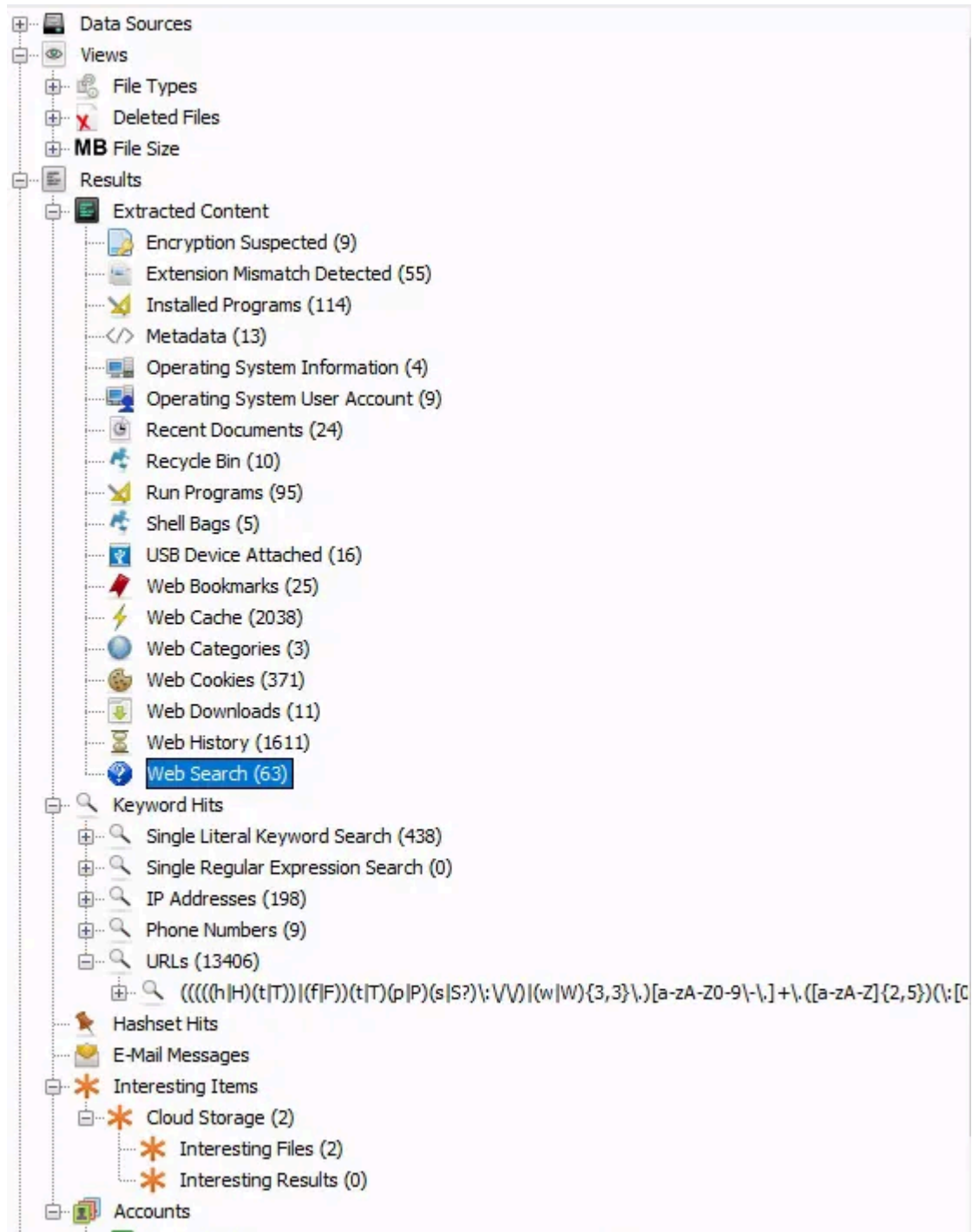
Page: 1 of 1 Page Matches on page: 1 of 5 Match 100% Reset

(secret\_project)\_pricing\_decision.xlsx.lnk \\10.11.11.128\Secured\_DRIVESecret P  
 oject Data\pricing decision  
 1SPS0  
 10.11.11.128  
 1SPS:  
 1SPSsC  
 \\10.11.11.128\secured\_driveMicrosoft NetworkCompany's Secured Network Drive  
 SECRET~1  
 Secret Project Data

Answer: 10.11.11.128

4: What web search term has the most entries?

I looked around and saw "Web Search" which may be something we need.



Once you click on Web Search, the right-hand side should show you what text was entered in a search engine. Look for one that shows up the most.



Listing Keyword search 4 - SECRET x

Web Search 63 Results

Table Thumbnail Summary

Save Table as CSV

Source File	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
index.dat				google.com	int	Internet Explorer	2015-03-22 22:09:43 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:03:40 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:05:18 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:05:19 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:05:22 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:05:48 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:06:27 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:14:50 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:15:44 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:16:55 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:17:14 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:18:10 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:18:15 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:18:30 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:18:43 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 18:18:46 GMT	sample-case.dd
History				google.com	information leakage cases	Google Chrome	2015-03-23 19:47:43 GMT	sample-case.dd

Answer: information leakage cases.

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

This time, we need to look at the “Date Accessed” column to help get our answer.

Web Search 63 Results

Table Thumbnail Summary

Save Table as CSV

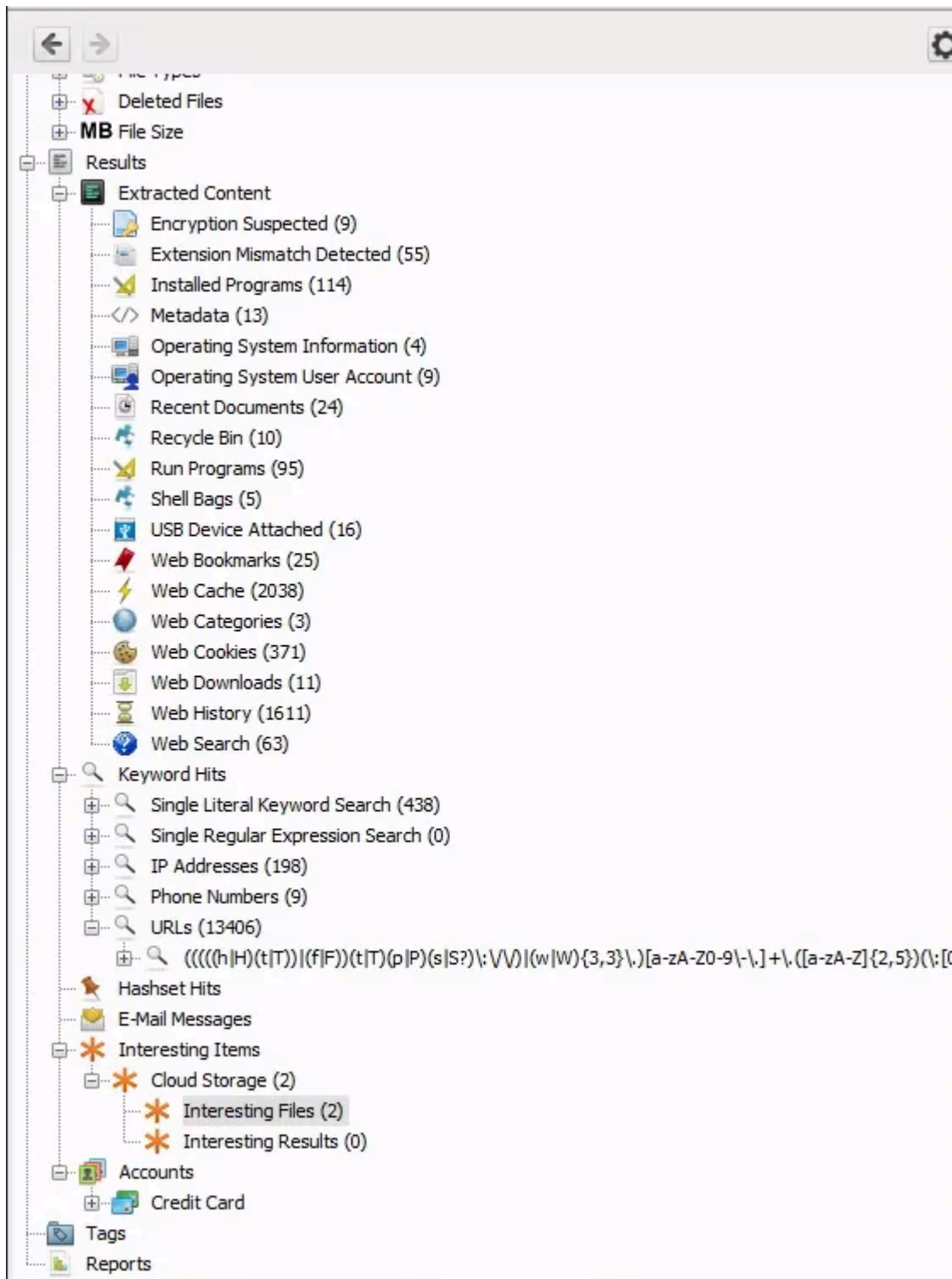
Source File	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat				bing.com	DLP DRM	Microsoft Edge	2015-03-24 01:08:31 GMT	sample-case.dd
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge	2015-03-24 01:08:54 GMT	sample-case.dd
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge	2015-03-24 01:09:31 GMT	sample-case.dd
WebCacheV01.dat				bing.com	Forensic Email Investigation	Microsoft Edge	2015-03-24 01:10:03 GMT	sample-case.dd
WebCacheV01.dat				bing.com	what is windows system artifacts	Microsoft Edge	2015-03-24 01:10:27 GMT	sample-case.dd
WebCacheV01.dat				bing.com	investigation on windows machine	Microsoft Edge	2015-03-24 01:11:50 GMT	sample-case.dd
WebCacheV01.dat				bing.com	windows event logs	Microsoft Edge	2015-03-24 01:12:35 GMT	sample-case.dd
WebCacheV01.dat				bing.com	cd burning method	Microsoft Edge	2015-03-24 01:13:20 GMT	sample-case.dd
WebCacheV01.dat				bing.com	cd burning method in windows	Microsoft Edge	2015-03-24 01:13:37 GMT	sample-case.dd
WebCacheV01.dat				bing.com	file sharing and tethering	Microsoft Edge	2015-03-24 01:13:58 GMT	sample-case.dd
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge	2015-03-24 01:14:11 GMT	sample-case.dd
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge	2015-03-24 03:43:47 GMT	sample-case.dd
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge	2015-03-24 03:43:52 GMT	sample-case.dd
WebCacheV01.dat				bing.com	anti-forensic tools	Microsoft Edge	2015-03-25 21:46:44 GMT	sample-case.dd
WebCacheV01.dat				bing.com	anti-forensic tools	Microsoft Edge	2015-03-25 21:46:44 GMT	sample-case.dd
WebCacheV01.dat				bing.com	eraser	Microsoft Edge	2015-03-25 21:46:54 GMT	sample-case.dd
WebCacheV01.dat				bing.com	ccleaner	Microsoft Edge	2015-03-25 21:47:51 GMT	sample-case.dd

Hex Text Application File Metadata Context Results Annotations Other Occurrences

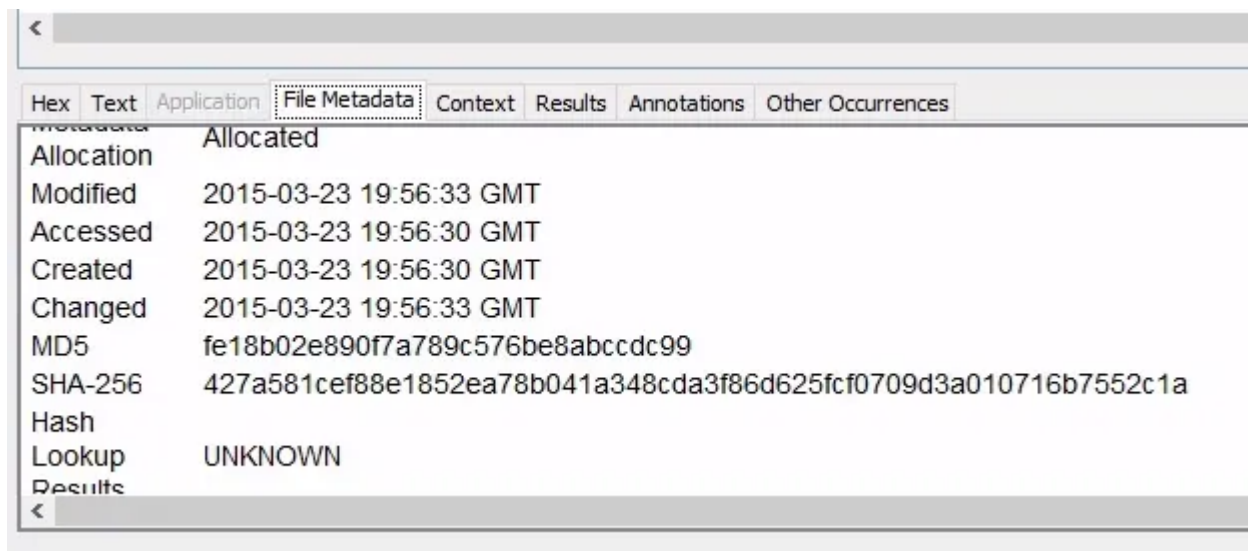
Answer: anti-forensic tools

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

Head on over to “Interesting Files” located under “Interesting Items.”



There are two files. Click on one of them and then look at the bottom and copy the hash. There's only two files, so 50% chance to get it right. With my luck, I got it on my second try.



The screenshot shows the Autopsy interface with the 'File Metadata' tab selected. The file being viewed is named 'Allocated'. The metadata fields and their values are as follows:

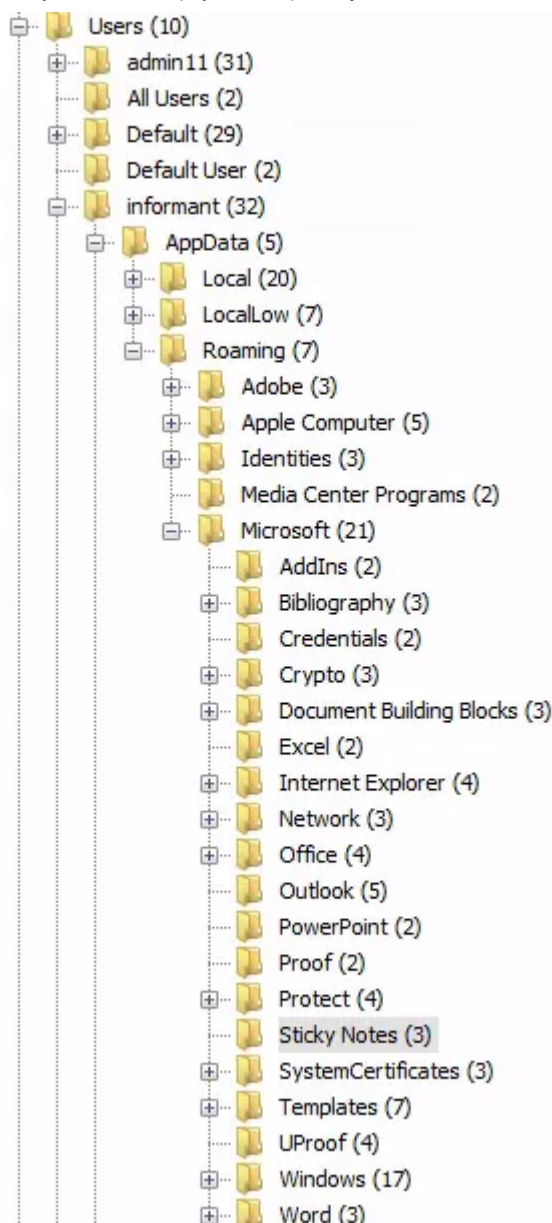
Field	Value
Allocation	Allocated
Modified	2015-03-23 19:56:33 GMT
Accessed	2015-03-23 19:56:30 GMT
Created	2015-03-23 19:56:30 GMT
Changed	2015-03-23 19:56:33 GMT
MD5	fe18b02e890f7a789c576be8abccdc99
SHA-256	427a581cef88e1852ea78b041a348cda3f86d625fcf0709d3a010716b7552c1a
Hash	
Lookup	UNKNOWN

Answer: fe18b02e890f7a789c576be8abccdc99

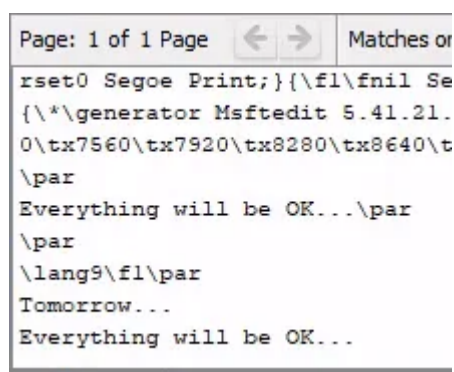
7: What self-assuring message did the 'Informant' write for himself on a Sticky Note?  
(no spaces)

I had a hard time with this. I searched multiple terms such as "StickyNotes" and "Informant" and had no luck. I also checked Informant's Desktop and Documents but did not find anything. I resorted to the same video once again. It looks like I was on the right track when trying to find Documents.

It seems like I had to navigate to Sticky Notes folder in the informant folder. So the path will be Data Sources -> sample-case.dd -> vol3 -> Users -> informant -> AppData -> Roaming -> Microsoft -> Sticky Notes.



Once there, you will see StickyNotes.snt. I'm not sure why me searching "StickyNotes" showed no results though. Once you selected the .snt file, look at the bottom and find the message.



Answer: Tomorrow... Everything will be OK...

## Task 8 Visualisation Tools

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

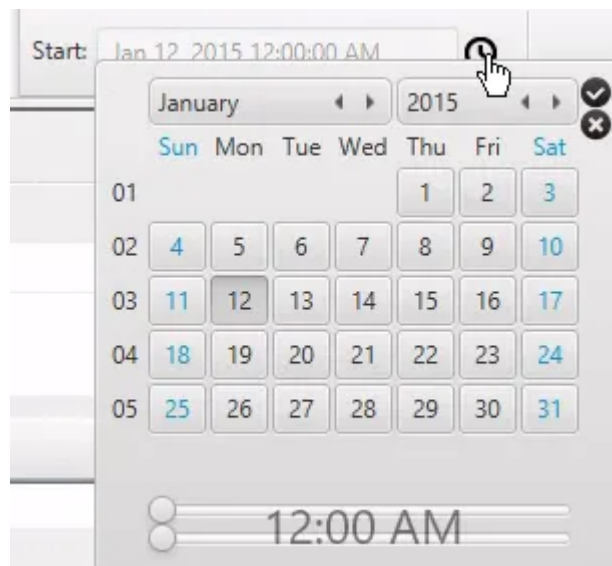
Open the timeline by clicking “Timeline” at the top.



I switched my mode to “Details” since I liked how it displayed in the readings more.

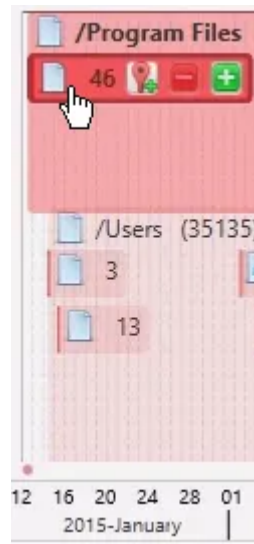


I clicked on the clock icon to adjust the date I want. It may take a while to set it properly. It took me a few tries.



After that, I hovered over the number 46 because it looks like there were 46 events that happened on January 15, 2015. I hovered over it until the information box came out to confirm the date.



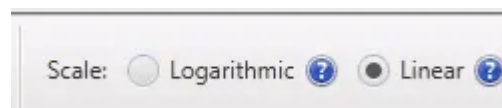


Answer: 46

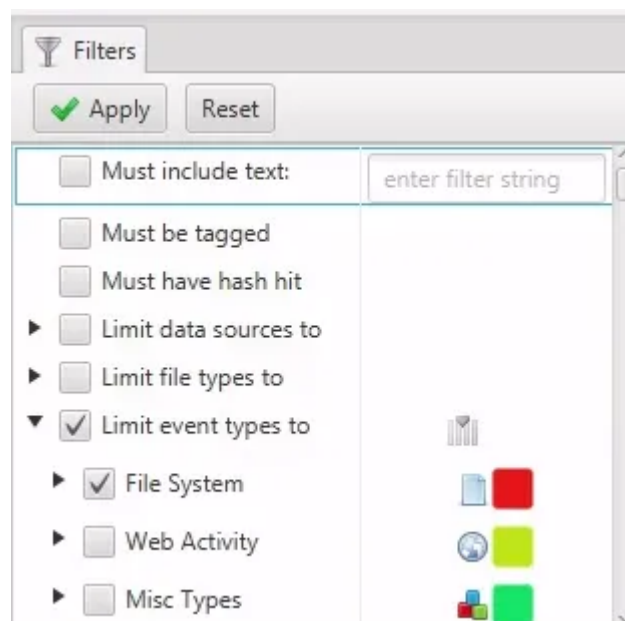
2: The majority of file events occurred on what date? (MONTH DD, YYYY)

This took me a bit of playing around. First, I changed the view back to “Counts.”

Next, I changed the scaling of the bar graphs into Linear.



On the left side, I changed the filters to show only events that deals with File Systems.

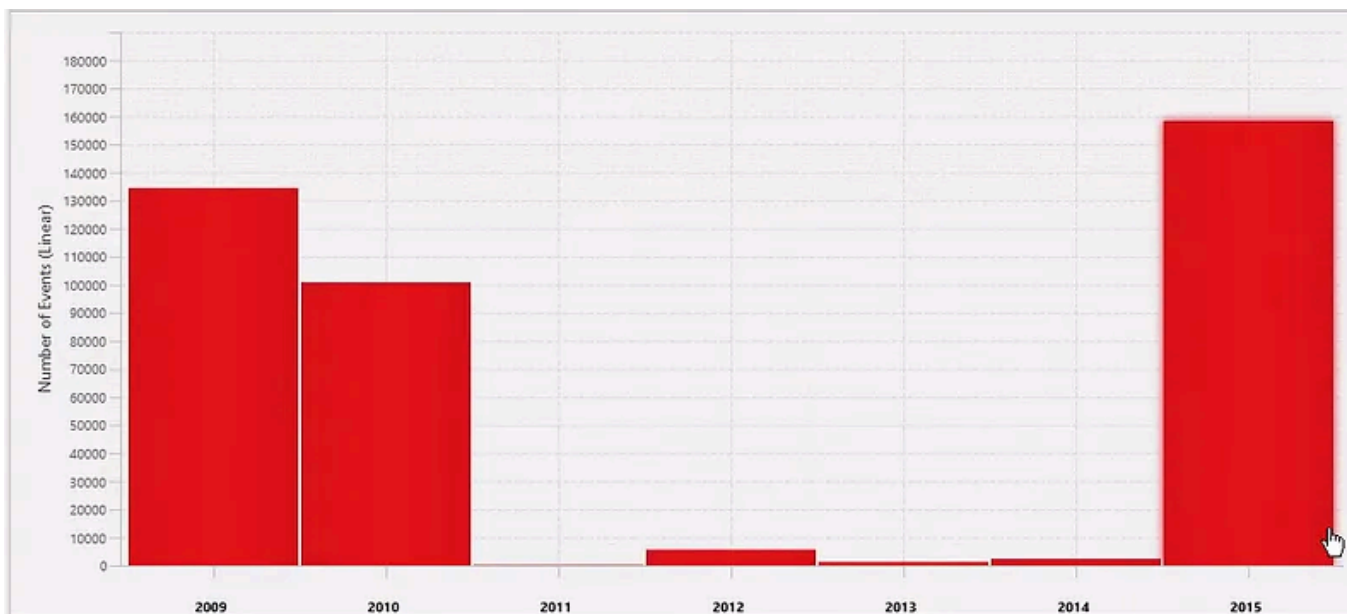


In the middle, I changed to show the entire timeline.

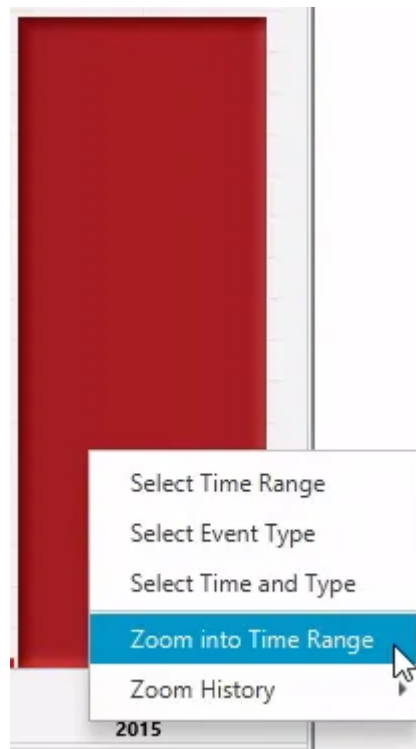




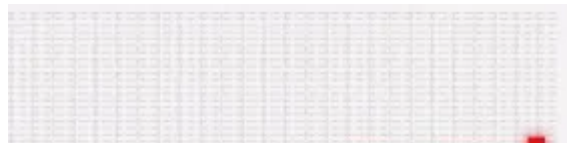
With that, it was just a matter of me choosing which bar was the taller one.



Right click the bar graph and select “Zoom into Time Range.”



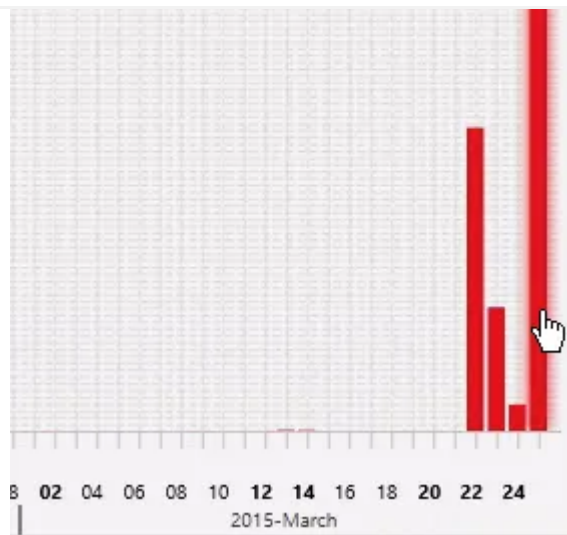
Then I just did it again.



[Open in app](#) ↗

Medium

Search



I'm not sure if it's proper but it works!

Answer: March 25, 2015

Thoughts:

Wow that was definitely challenging that I had to use external sources for help in a long time! As mentioned before, I will always post when I looked up for help because I want to show that I'm always learning, even if I am doing write-ups. I do wonder why "StickyNotes" didn't result in "StickyNotes.snt" popping up when I searched it. I'm really interested in doing the challenge room but I might have to do that in the future. I'm very close to finishing the SOC Level 1 path that I want to just focus on that first! Just a few more rooms!

Cybersecurity

Tryhackme

Autopsy

Dfir

Digital Forensics



Follow

## Written by Toumo

152 Followers · 1 Following

## Responses (1)



What are your thoughts?

Respond



Samar

about 2 months ago



thanks



Reply

## More from Toumo

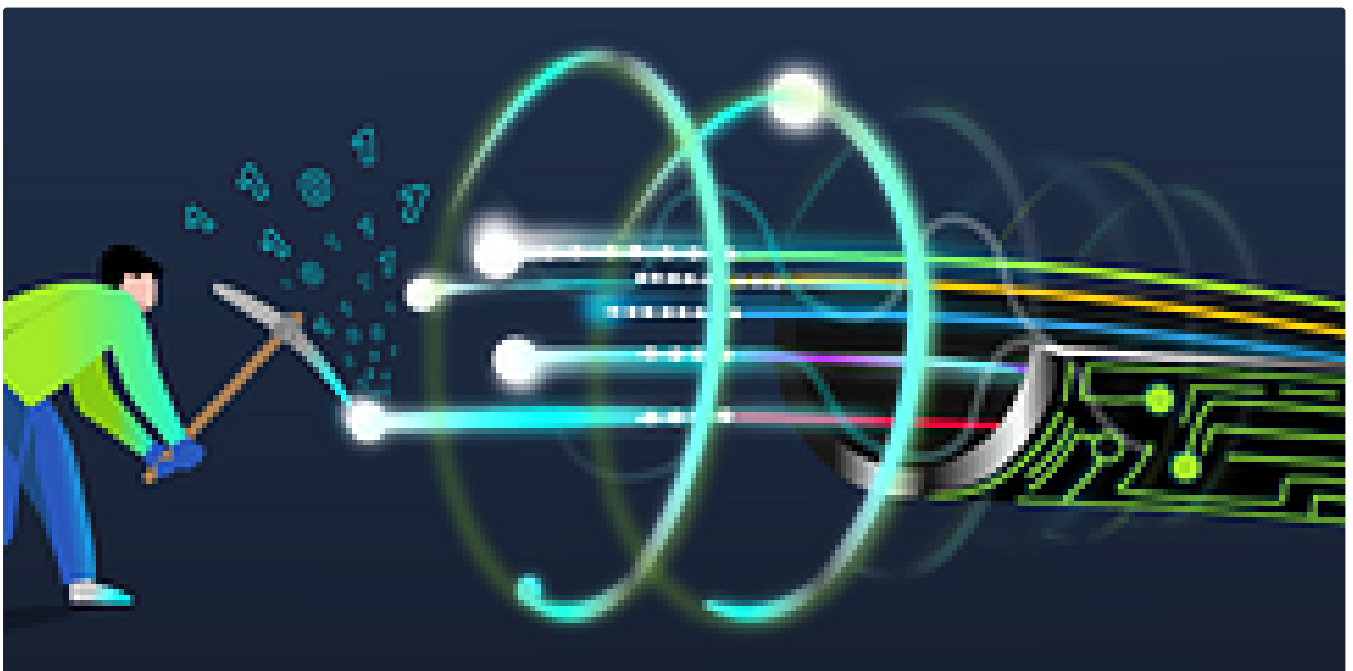


T Toumo

### TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023 🖱 20 💬 1





Toumo

## TryHackMe NetworkMiner Write-Up

This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what...

Jul 5, 2023



6



1



Toumo

## TryHackMe Sysmon Write-Up

We will be doing the Sysmon room this time. I don't know about Sysmon too much except that it's usually running in the background and helps...

Jul 31, 2023



6





T Toumo

## TryHackMe TheHive Project Write-Up

I don't know why, but the idea of having multiple people working on a case simultaneously sounds pretty cool. It's like working on Google...

Aug 9, 2023 🖱 11



See all from Toumo

## Recommended from Medium



```
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc   run    snap sys  usr    vmlinuz

var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd          unattended-upgrades
cloud-init.log         fontconfig.log  landscape     syslog       wtmp
dist-upgrade          journal       lastlog      tallylog

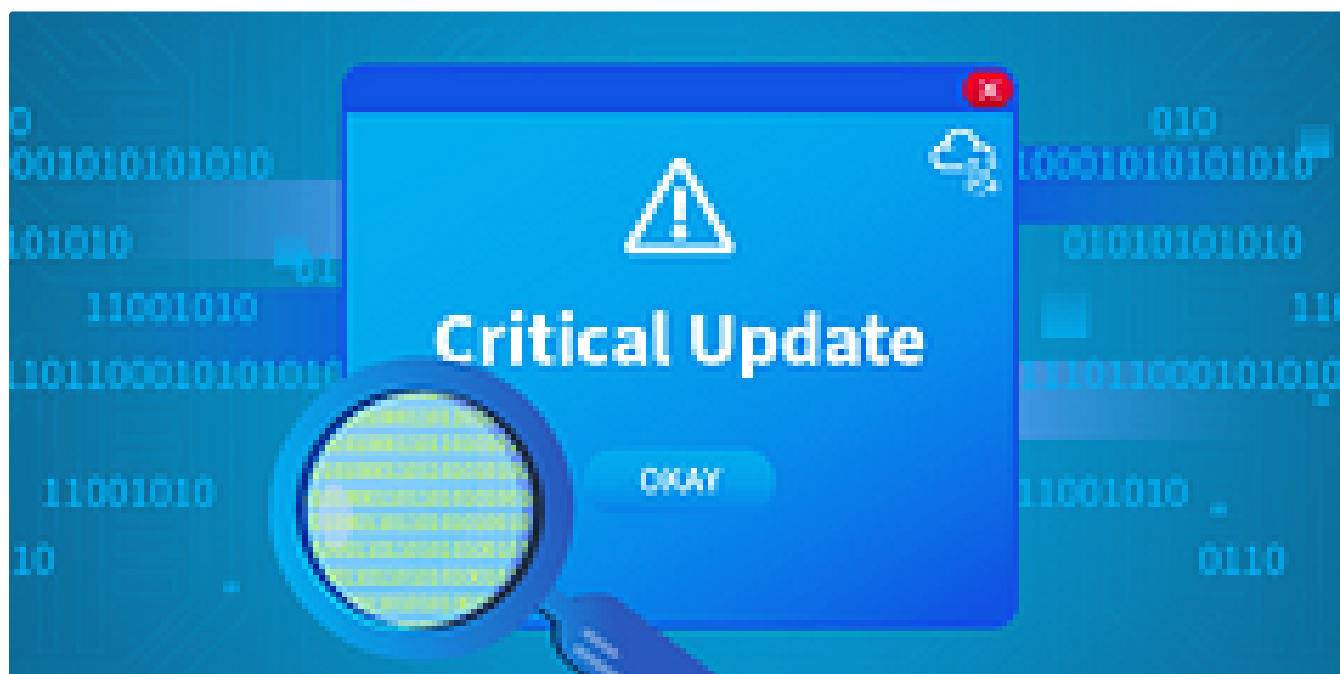
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PwD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PwD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PwD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

T Dan Molina

## Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:  
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



In T3CH by Axoloth

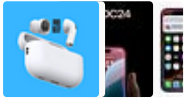
## TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

★ Jul 21, 2024 🖱 104



## Lists



### Tech & Tools

22 stories · 380 saves



### Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves



### Staff picks

796 stories · 1561 saves



### Natural Language Processing

1884 stories · 1529 saves



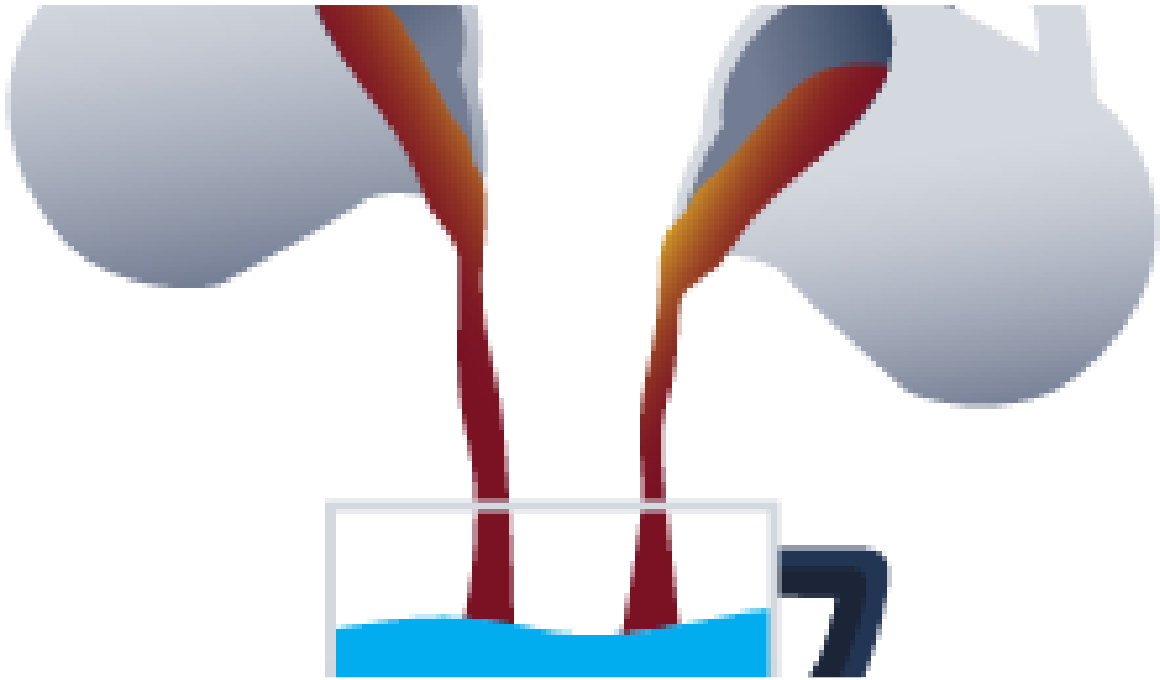
In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60





 MAGESH

## Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024  2



Try Hack Me


NEW CHALLENGE ROOM!

# Disgruntled

Use your Linux forensics knowledge to investigate an incident

[tryhackme.com/room/disgruntled](https://tryhackme.com/room/disgruntled)

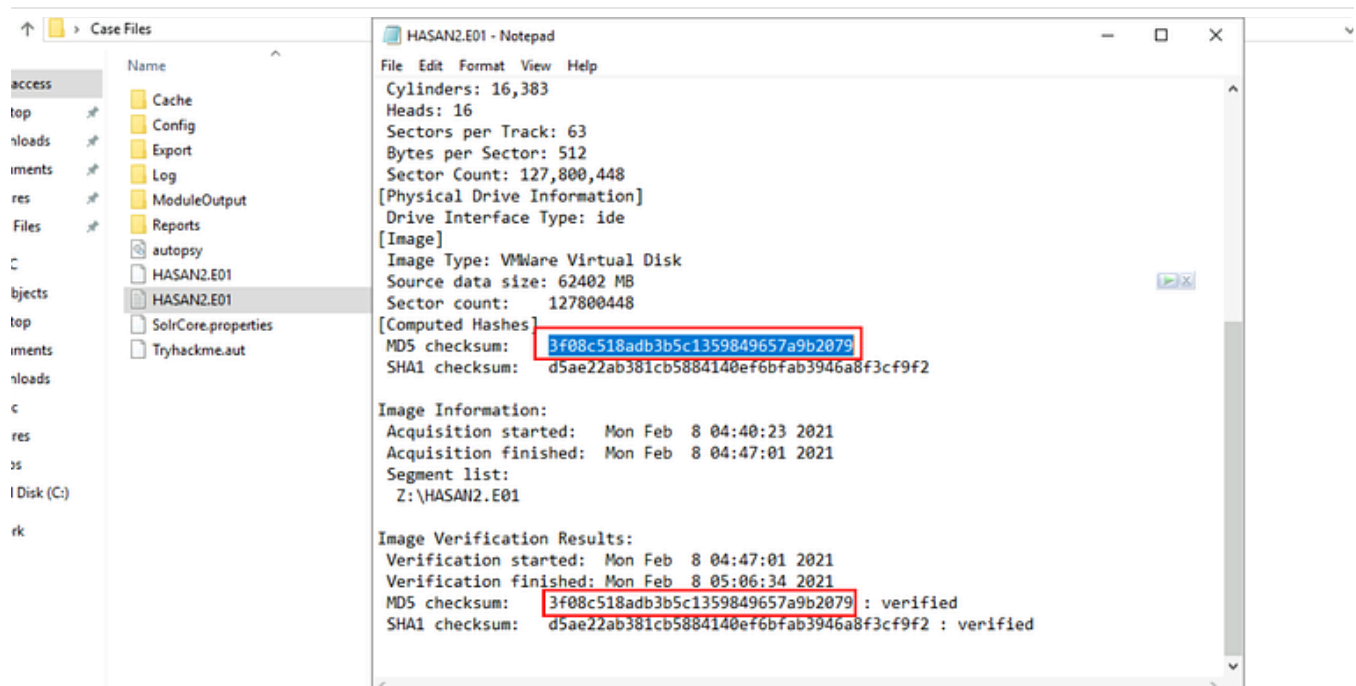
Difficulty: **Easy** Platform: **Linux**

 Mustapha Ait Ichou

## Disgruntled Tryhackme

Hi All, i hope you are doing well thank for taking your time to read my writup i hope it's will be useful for you. In this write-up, I will...

Aug 14, 2024



Chicken0248

## [TryHackMe Write-up] Disk Analysis & Autopsy

Ready for a challenge? Use Autopsy to investigate artifacts from a disk image.

Sep 14, 2024

[See more recommendations](#)