

Autopsy

Task 2 Workflow Overview and Case Analysis

What is the file extension of the Autopsy files?

.aut

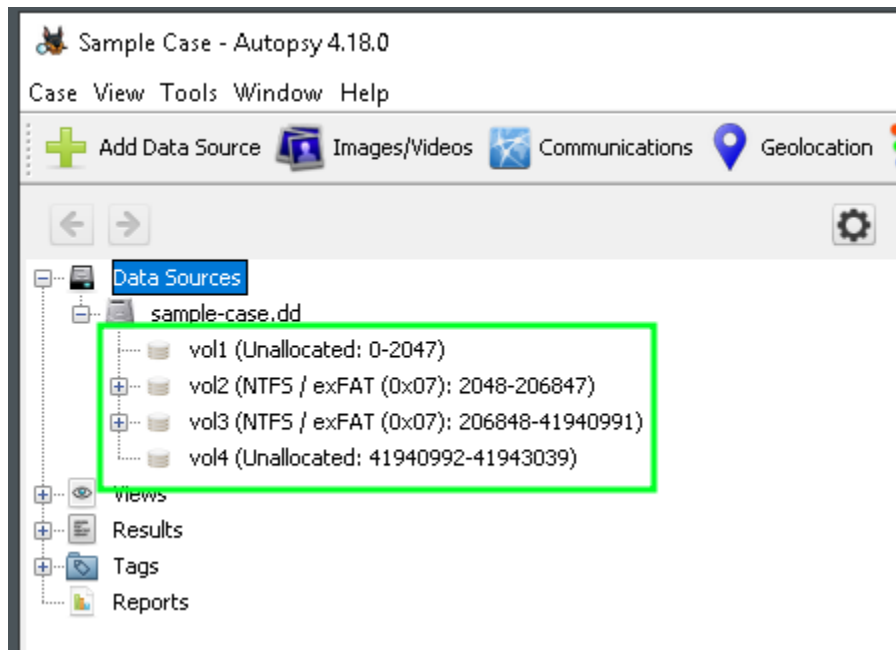
Task 3 Data Sources

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**

Source File	S	C	O	Path	Time Deleted	Username	Data Source
\$RKXD1U3.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$R13FM2A.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$R1QGWT7T.ini				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$R508CB6.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$R3JMT64.exe				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us....	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$R8YF3XK.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$RUSPKWT.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$RX38VH.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$RFVQHSV.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd
\$RDOI3HE.jpg				C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg	2015-03-24 20:11:42 GMT	informant	sample-case.dd

10

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

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

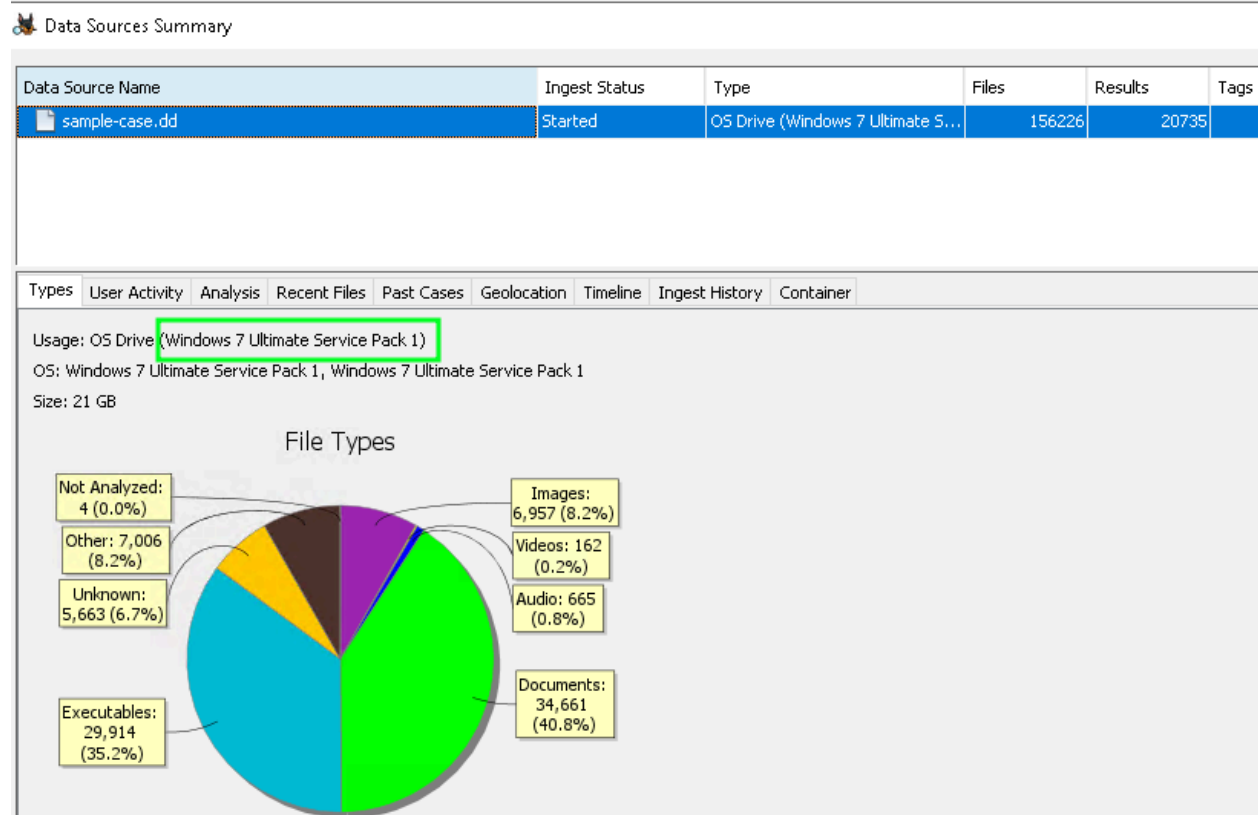
Source File	S	C	O	Category	File Path
googledrivesync.exe			0	Google Drive	/img_sample-case.dd/vol_vol3/Users/informant/Downloads/googledrivesync.exe
googledrivesync.exe			0	Google Drive	/img_sample-case.dd/vol_vol3/Program Files (x86)/Google/Drive/googledrivesync.exe

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

Job 10:

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

1-1-11

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

DirectoryTree	2009-07-14 11:53:25 GMT /img_sample-case.dd/vol3/windows/System32/config/SOFTWARE
Eraser 6.2.0.2962 v6.2.2962	2015-03-25 21:57:31 GMT /img_sample-case.dd/vol3/Windows/System32/config/SOFTWARE
Fontcore	2009-07-14 11:53:25 GMT /img_sample-case.dd/vol3/Windows/System32/config/RegBack/SOFTWARE

Eraser

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

Search for the Password Hint in the keyword search section

Page: 1 of 1 Page	Matches on page: 1 of 1 Match	100%	Re:
User ID : S-1-5-21-2425377081-3129163575-2985601102-1000			
Username : informant			
Date Created : 2015-03-22 14:33:54 GMT			
Date Accessed : 2015-03-25 13:06:08 GMT			
Count : 9			
Account Type : Default Admin User			
Password Hint : IAMAN			
Password Fail Date : 2015-03-22 15:57:48 GMT			
Password Settings : Password does not expire, Password not required			
Flag : Normal user account			

IAMAN

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

Search for the secret

Name	Keyword Preview	Location	Modified Time	Change Time
Web History Artifact	URL: file:///E:/<Secret*>20Project%20Data/design/vi	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-25 15:30:56 GMT	2015-03-25 15:30:56 GMT
(secret_project)_pricing_decision.xlsx.LNK	Secured Network Drive<SECRET*>1<Secret* Project Data...	/img_sample-case.dd/vol3/Users/informant/AppData/R...	2015-03-23 20:26:53 GMT	2015-03-23 20:26:53 GMT
V0100024.log	Visited: informant@file:///E:/<Secret*>20Project%20Data...	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-25 14:46:07 GMT	2015-03-25 14:46:07 GMT
1b4dd67f29cb1962.automatDestinations-ms	V/<Secret* Project Data/f/V/<Secret*>20Project%20Data...	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-25 15:28:47 GMT	2015-03-25 15:28:47 GMT
Local State	"cohort_seed": 299, "secret*": "q/ek7evYyHwId8b8	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-24 21:07:21 GMT	2015-03-24 21:07:21 GMT
V0100025.log	11.11.128(secured_drive)<Secret*>20Project%20Data/pric	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-25 14:47:30 GMT	2015-03-25 14:47:30 GMT
47bb2136fda3f1ed.automatDestinations-ms	7295<secret*en-US<secret*en-USsecretD<secret*en-US	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-25 15:29:08 GMT	2015-03-25 15:29:08 GMT
r_000022	<a href="/search?q=<Secret*>Naaz+hideout&am...	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-22 15:12:12 GMT	2015-03-22 15:12:12 GMT
History Provider Cache	ssetlemillonleak<secret*>0btdgaboutafqcnf7	/img_sample-case.dd/vol3/Users/informant/AppData/...	2015-03-24 21:07:20 GMT	2015-03-24 21:07:20 GMT

```

(secret_project)_pricing_decision.xlsx.LNK \\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\secret_project_pricing_decision.xlsx\\10.11.11.128\secured_drive\
18PB0
10.11.11.128
18PB:
18PB:c
\\10.11.11.128\secured_drive\Microsoft Network\Company's Secured Network Drive
SECRET-1
Secret Project Data
PRICIN-1
pricing decision
(S2EBP-1.XLS
(secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\secret_project_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\secret_project_pricing_decision.xlsx
18PB
  
```

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	google.com	2015-03-23 18:05:18 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:05:19 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:05:22 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:05:48 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:06:27 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:14:50 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:15:44 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:16:55 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:17:14 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:18:10 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:18:15 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
information leakage cases	google.com	2015-03-23 18:18:30 GMT	Google Chrome	/img_sample-case.dd/vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History

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	bing.com	2015-03-25 21:46:44 GMT Mi
anti-forensic tools	bing.com	2015-03-25 21:46:44 GMT Mi
apple icloud	google.com	2015-03-23 18:55:09 GMT G

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

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_sample-case.dd/vol_vol3/Users/informant/Downloads/google drivesync.exe						
Type	File System						
MIME Type	application/x-dosexec						
Size	880208						
File Name	Allocated						
Allocation	Allocated						
Metadata	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						
Results							
Internal ID	13894						
Downloaded From	http://dl.google.com/tag/s/appguid%3D%7B3C122445-AECE-4309-90B7-85A6AEF42AC0%7D%26iid%3D%7B135CA63f						

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

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
[current folder]				2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	272	Allocated	Allocated	unknown	/in
[parent folder]				2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	2015-03-22 14:34:41 GMT	56	Allocated	Allocated	unknown	/in
StickyNotes.snt			0	2015-03-24 18:31:59 GMT	2015-03-24 18:31:59 GMT	2015-03-24 18:30:09 GMT	2015-03-24 18:30:09 GMT	4096	Allocated	Allocated	unknown	/in

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Sou

```

Root Entry
Version
Metafile
ccbb72fb-d253-11e4-b
ccbb72fb-d253-11e4-b
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fs22\
rset0 Segoe Print;}{\f1\fnil Segoe Print;}}
{\*\generator Msftedit 5.41.21.2510;}{viewkind4\uc1\pard\tx360\tx720\tx1080\tx1440\tx1800\tx2160\tx2520\tx2880\tx3240\tx3600\tx3960\tx4320\tx4680\tx5040\tx5400\tx5760\tx6120\tx6480\tx6840\tx7200\tx7560\tx7920\tx8280\tx8640\tx9000\tx9360\tx9720\tx10080\tx10440\tx10800\tx11160\tx11520\highlight0\fs22 Tomorrow...}\par
\par
Everything will be OK...\par
\par
\lang0\fs22\par
Tomorrow...
Everything will be OK...

```

Tomorrow...Everything will be OK...

Task 8 Visualisation Tools

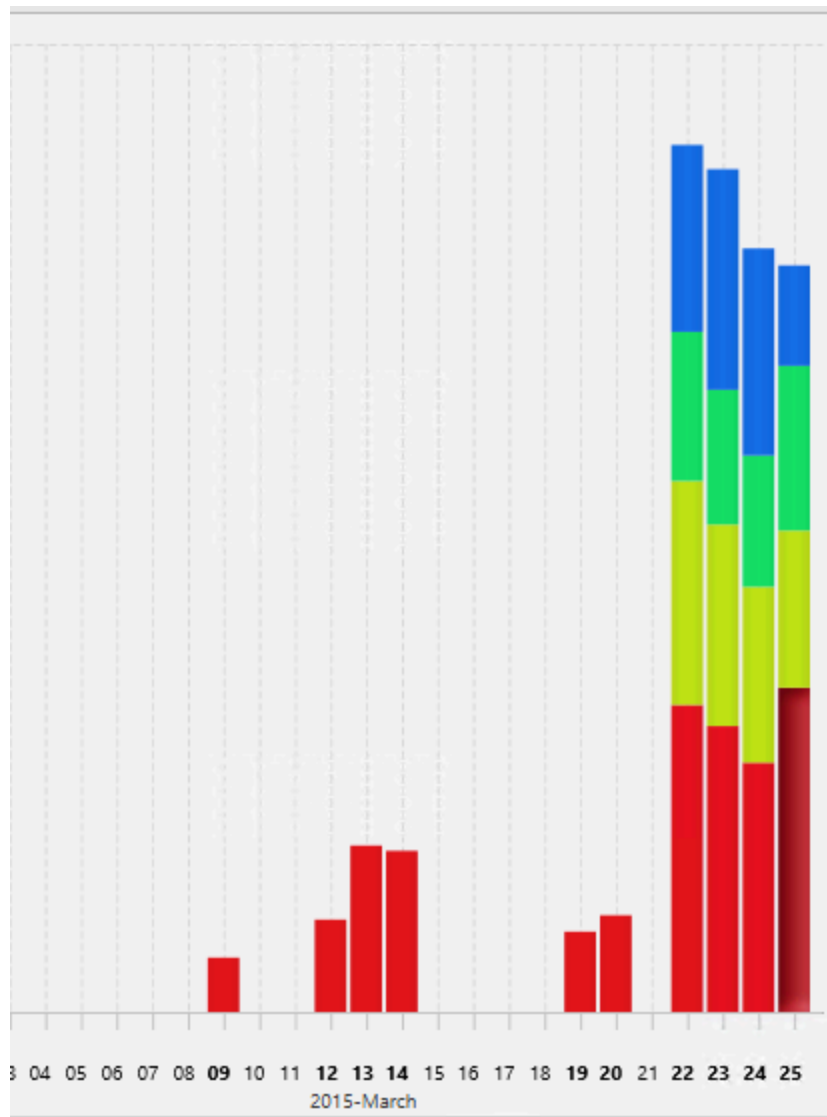
Using the Timeline, how many results were there on 2015-01-12?

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