

Data Science for Digital Forensics & Incident Response

ODSC West '21 - Workshop

Jess Garcia

One eSecurity – Founder | SANS – Senior Instructor

jess@one-esecurity.com -  @j3ssgarcia

\$ whoami



Jess Garcia

@j3ssgarcia



Founder and CEO of One eSecurity, a global Digital Forensics and Incident Response (DFIR) company (~15 years).



Leader of the DS4N6 project.
Visit: www.ds4n6.io



Senior Instructor at the SANS Institute (~20 years).


DFIR




SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

f SANSForensics dfr.to/DFIRCast
@SANSForensics

OPERATING SYSTEM & DEVICE IN-DEPTH

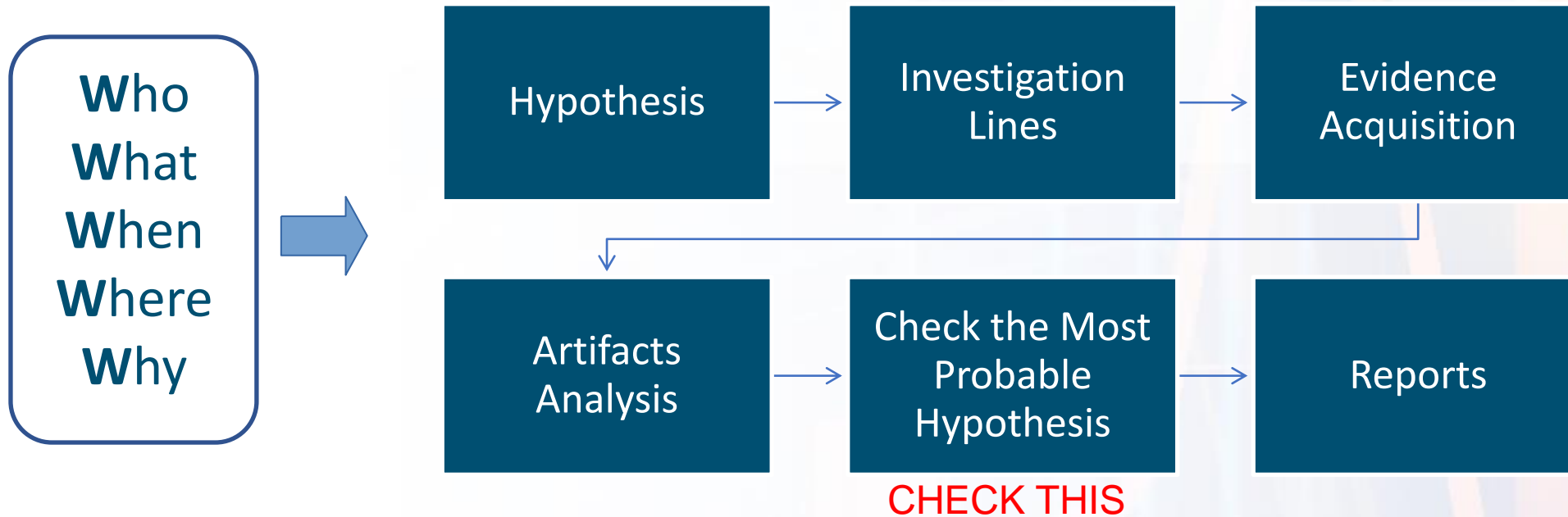
-  **FOR308**
Digital Forensics Essentials
-  **FOR498**
Battlefield Forensics & Data Acquisition
GBFA
-  **FOR500**
Windows Forensic Analysis
GCFE
-  **FOR518**
Mac and iOS Forensic Analysis & Incident Response
-  **FOR585**
Smartphone Forensic Analysis In-Depth
GASF

INCIDENT RESPONSE & THREAT HUNTING

-  **FOR508**
Advanced Incident Response, Threat Hunting, & Digital Forensics
GCFA
-  **FOR572**
Advanced Network Forensics: Threat Hunting, Analysis, & Incident Response
GNFA
-  **FOR578**
Cyber Threat Intelligence
GCTI
-  **FOR610**
REM: Malware Analysis Tools & Techniques
GREM
-  **SEC504**
Hacker Tools, Techniques, Exploits, & Incident Handling
GCIH

Forensic Investigation

Answer the 5Ws



Windows Artifacts Categories

File Download

- Open/Save MRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Outlook
- E-mail Attachments**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Outlook
- Skype History**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Skype
- Index.dat/ Places.sqlite**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Internet Explorer
- Downloads.sqlite**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Firefox

Program Execution

- UserAssist**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: UserAssist
- Last Visited MRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Internet Explorer
- RunMRU Start-Run**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: RunMRU
- Application Compatibility Cache**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Application Compatibility Cache
- Win7 Jump Lists**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Win7 Jump Lists
- Prefetch**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Prefetch
- Services Events**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Services Events

File Opening / Creation

- Open/Save MRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Outlook
- Last Visited MRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Internet Explorer
- Recent Files**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Recent Files
- Office Recent Files**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Office Recent Files
- Shell bags**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Shell bags
- Shortcut (LNK) Files**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Shortcut (LNK) Files
- Win7 Jump Lists**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Win7 Jump Lists
- Prefetch**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Prefetch
- Index.dat file/**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Index.dat file/

Deleted File or File Knowledge

- XP Search -ACMRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: XP Search -ACMRU
- Win7 Search - WordWheel Query**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Win7 Search - WordWheel Query
- Last Visited MRU**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Last Visited MRU
- Thumbs.db**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Thumbs.db
- Vista/Win7 Thumbnails**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Vista/Win7 Thumbnails
- XP Recycle Bin**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: XP Recycle Bin
- Win7 Recycle Bin**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Win7 Recycle Bin
- Index.dat file/**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Index.dat file/

Physical Location

- Timezone**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Timezone
- VISTA/Win7 Network History**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: VISTA/Win7 Network History
- Cookies**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Cookies
- Browser Search Terms**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Browser Search Terms

USB or Drive Usage

- Key Identification**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Key Identification
- First / Last Times**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: First / Last Times
- User**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: User
- Volume Serial Number**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Volume Serial Number
- Drive Letter and Volume Name**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Drive Letter and Volume Name
- Shortcut (LNK) Files**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: Shortcut (LNK) Files
- P&P Event Log**: Description: The MRU list shows the files that have been opened or saved in the application. The location of the file is listed in the MRU list. Location: P&P Event Log

Created for FOR408 - Windows Forensics - SANS Digital Forensics and Incident Response faculty created the "Evidence of..." categories to map a specific artifact to the analysis question that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key items to an activity for Microsoft Windows systems for intrusions, intellectual property theft, or common cyber-crimes.

Proper digital forensic and incident response analysis is essential to successfully solving complex cases today. Each analyst should examine the artifacts and then analyze the activity that they describe to determine a clear picture of which user was involved, what the user was doing, when they were doing it, and why. The data here will aid you in finding multiple locations that can help substantiate facts related to your casework.

Account Usage

- Last Login**: Description: Lists the local accounts of the system and their expiration dates. Location: Local
- Last Password Change**: Description: Lists the last time the password of a specific user has been changed. Location: Local
- Success / Fail Logons**: Description: Describes which accounts have been used for attempted logons. Location: Local
- Logon Types**: Description: Logon events can give us very specific information regarding the nature of account authentication systems if we know where to look and how to decipher the data that we find. Location: Local
- RDP Usage**: Description: Track Remote Desktop Protocol logs to target machines. Location: Security Log

Browser Usage

- History**: Description: Lists the URLs visited by the user. Location: Internet Explorer
- Cookies**: Description: Lists the cookies stored by the browser. Location: Internet Explorer
- Cache**: Description: Lists the cache files stored by the browser. Location: Internet Explorer
- Session Restore**: Description: Lists the session restore files stored by the browser. Location: Internet Explorer
- Flash & Super Cookies**: Description: Lists the Flash and Super Cookies stored by the browser. Location: Internet Explorer

Each of the rows listed will describe a series of artifacts found on a Windows system to help determine if that action occurred. Usually multiple artifacts will be discovered that will all point to the same activity. These locations are a guide to help you focus your analysis in the right areas in Windows that could aid you in answering simple questions.



Download the SANS poster here: <https://www.sans.org/posters/windows-forensic-analysis/>

Windows Forensic Tools

plaso

- Parse logs and artifacts
- Correlated supertimeline

<https://github.com/log2timeline/plaso>



fls & mactime

- FLS: lists files and directories
- Mactime: timeline based on FLS

<https://github.com/sleuthkit/sleuthkit>




SANS Faculty DFIR Tools





Find more free SANS tools:
<https://www.sans.org/img/free-faculty-tools.pdf>

Other Open Source Tools



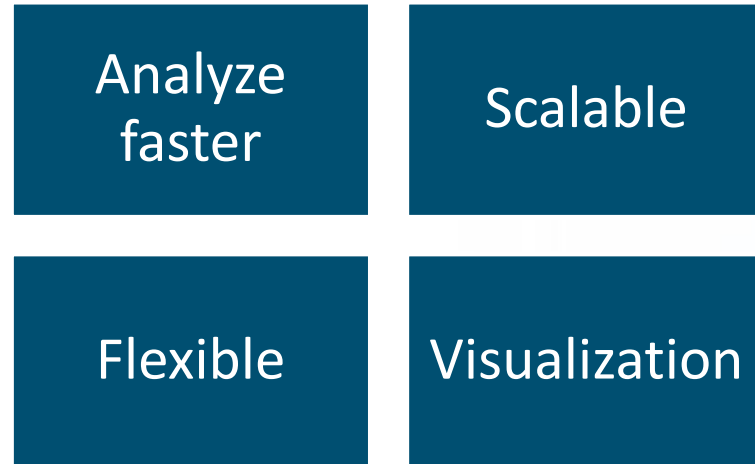



Comercial Tools





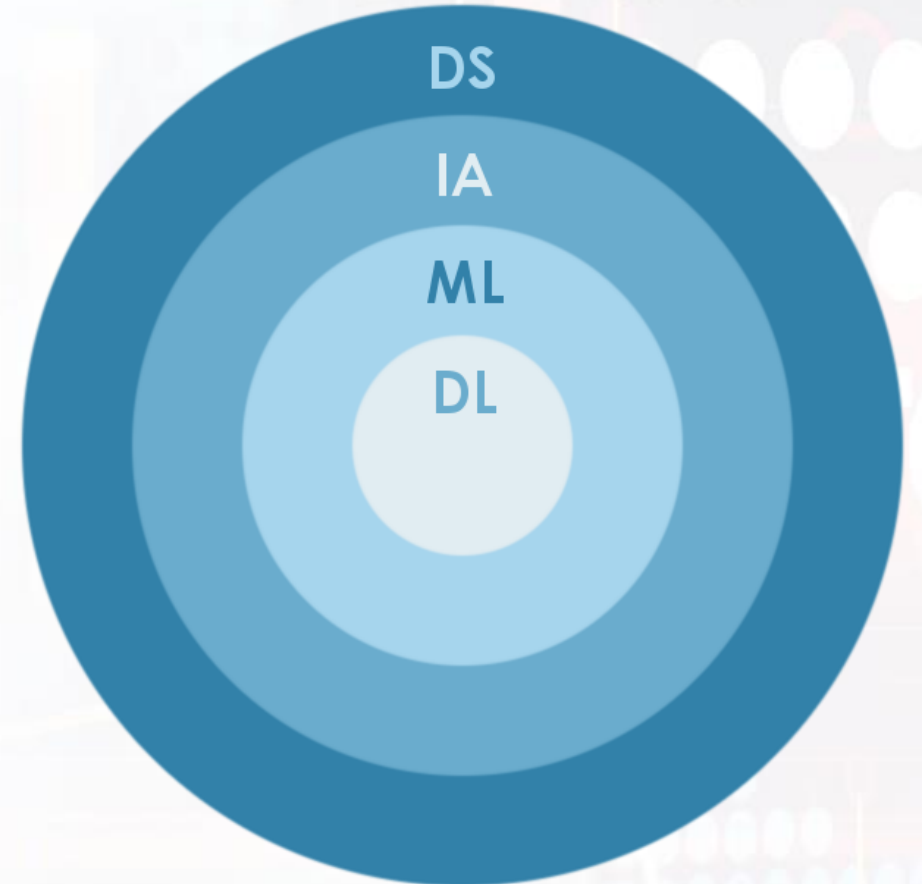
Intro to Data Science



Used in Finance, Medicine, Marketing, Retail...

And many more!

So... What about using it on DFIR?



Jupyterlab

File Edit View Run Kernel Tabs Settings Help

FAVORITES

- 0-links
- 0-links-neva-local
- 0-templates

FILE BROWSER

/ ... / 0-links / szechuan_ds4n6 /

Name	Last Modified
notebooks	a month ago

IMPORTS & INIT

```
[2]: # Data Science Imports
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt

# GUI Imports
import qgrid
from IPython.display import display, Markdown
#import ipynb_path

# Visualization
import matplotlib.pyplot as plt
import seaborn as sns
import pandas_bokeh
from bokeh.io import output_notebook, show
from bokeh.plotting import figure, output_file, show

# DFIR Imports
from timesketch_api_client import client
from timesketch_api_client import config
import timesketch_api_client

# DS4N6
import ds4n6.lib.d4 as d4
import ds4n6.lib.common as d4com
import ds4n6.lib.autoruns as d4atrs
import ds4n6.lib.fstl as d4fstl
import ds4n6.lib.plaso as d4pl
import ds4n6.lib.kansa as d4ksa
import ds4n6.lib.kape as d4kp
import ds4n6.lib.evtx as d4evtx
import ds4n6.lib.mactime as d4mctm
import ds4n6.lib.unx as d4unx
import ds4n6.lib.utils as d4util
import ds4n6.lib.gui as d4gui
import ds4n6.lib.ml as d4ml
import ds4n6.lib.tshark as d4tshrk
import ds4n6.lib.flist as d4flst

from ds4n6.lib.common import analysis
from ds4n6.lib.common import anl
from ds4n6.lib.common import whatis
from ds4n6.lib.common import find_anomalies
from ds4n6.lib.unx import xgrep
from ds4n6.lib.gui import xread
from ds4n6.lib.gui import xmenu
from ds4n6.lib.gui import xdisplay
from ds4n6.lib.gui import xanalysis

# Standard python imports
```

File Edit View Run Kernel Tabs Settings Help

find_anomalies_testing.ipynb × ml.py ×

FAVORITES

- 0-links
- 0-links-neva-local
- 0-templates

FILE BROWSER

/ ... / 0-links / szechuan_ds4n6 /

Name	Last Modified
notebooks	a month ago

```
Epoch 4/10
9406/9406 [=====] - 8s 867us/step - loss: 0.2824
Epoch 5/10
9406/9406 [=====] - 8s 857us/step - loss: 0.2283
Epoch 6/10
9406/9406 [=====] - 8s 851us/step - loss: 0.1840
Epoch 7/10
9406/9406 [=====] - 8s 837us/step - loss: 0.1492
Epoch 8/10
9406/9406 [=====] - 8s 846us/step - loss: 0.1231
Epoch 9/10
9406/9406 [=====] - 8s 812us/step - loss: 0.1044
Epoch 10/10
9406/9406 [=====] - 8s 830us/step - loss: 0.0918

- Training End: 2021-10-22 11:41:38

- Models: ['model_5']
- Losses: [0.09179588407278061]
- Min. Loss: 0.09179588407278061
- Min. Loss Model: model_5

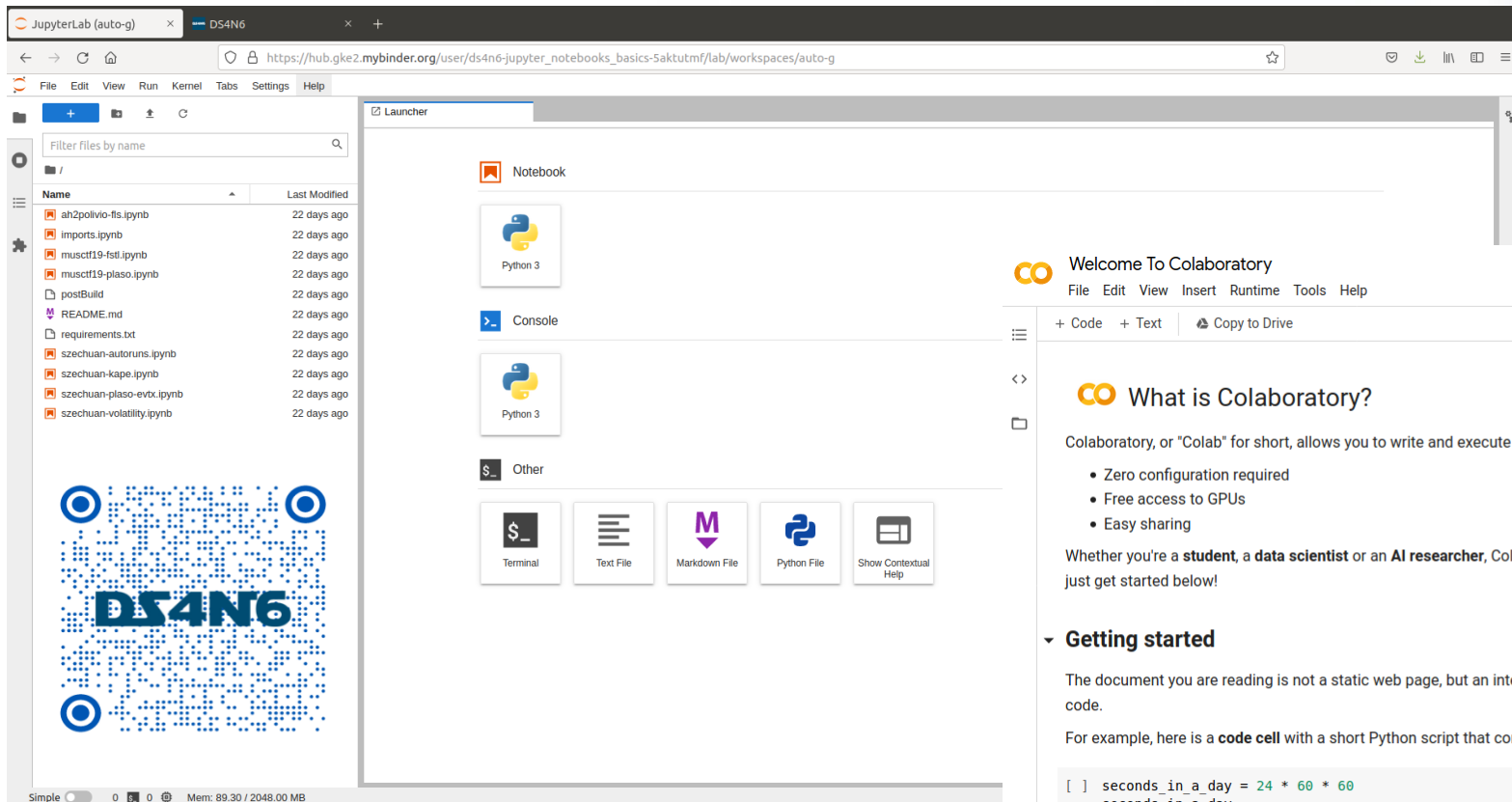
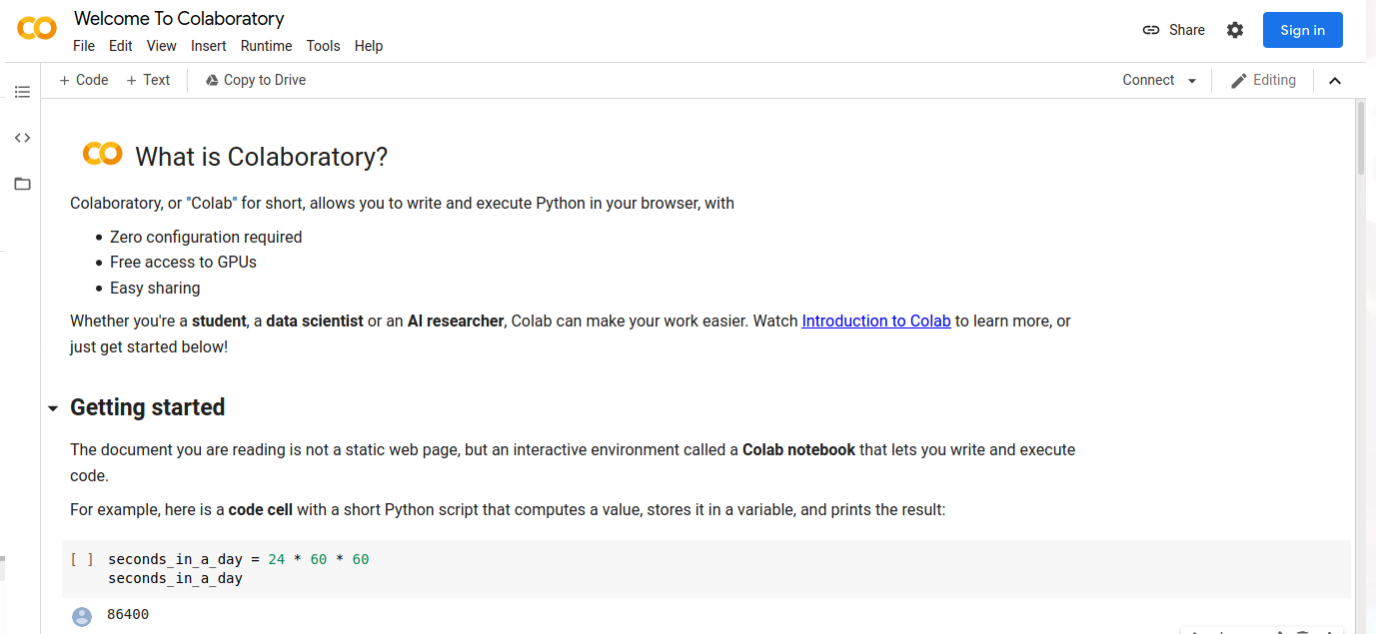
PREDICTIONS

- Setting autoencoder to min loss model: model_5
- Input DF Shape: (300964, 5) -> (300964, 5)
- Running predictions...
+ Start: 2021-10-22 11:41:38
+ End: 2021-10-22 11:41:41
None
- Error Threshold: 0 (Auto-calculated - Top 15)
- No.Anomalies: 300964
- RUN ID: 20211022114013
```

0 22 Python 3 | Idle

Saving completed

Doing DS on the Cloud: binder & colab

Visit bit.ly/3Ff2VOM Or scan the QR code to test the DS4N6 repository

Data Structures: Dataframes

```
df.head()
```

Timestamp	D4_DataType_	D4_Orchestrator_	D4_Tool_	D4_Plugin_	D4_Hostname_	EventRecordID	EventID_	evtFileName_	ProviderName	ProviderGuid	System > EventID	Version	Level	Task	Opcode	Keywords	ProcessID	Threa
2020-09-18 05:41:16	evtX	NaN	plaso	windows_evtX_record	NaN	16	4624	Security.evtX	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-A5BA-3E3B0328C30D}	4624	2	0	12544	0	0x8020000000000000	660	6
2020-09-18 05:41:17	evtX	NaN	plaso	windows_evtX_record	NaN	47	4624	Security.evtX	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-A5BA-3E3B0328C30D}	4624	2	0	12544	0	0x8020000000000000	660	7
2020-09-18 05:41:17	evtX	NaN	plaso	windows_evtX_record	NaN	50	4624	Security.evtX	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-A5BA-3E3B0328C30D}	4624	2	0	12544	0	0x8020000000000000	660	7
2020-09-18 05:41:18	evtX	NaN	plaso	windows_evtX_record	NaN	51	4624	Security.evtX	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-A5BA-3E3B0328C30D}	4624	2	0	12544	0	0x8020000000000000	660	7
2020-09-18 05:41:18	evtX	NaN	plaso	windows_evtX_record	NaN	54	4624	Security.evtX	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-A5BA-3E3B0328C30D}	4624	2	0	12544	0	0x8020000000000000	660	7

Data Structures: Dictionaries

```
pldfs_srv.keys()
```

```
dict_keys(['windows_registry_installation', 'windows_registry_userassist', 'windows_lnk_link', 'fs_stat', 'olecf_item', 'pe_compilation_compilation_time', 'windows_registry_key_value', 'windows_shell_item_file_entry', 'windows_distributed_link_tracking_creation', 'task_scheduler_task_cache_entry', 'windows_evtx_record', 'windows_registry_network', 'fs_ntfs_usn_change', 'setupapi_log_line', 'windows_registry_run', 'windows_registry_msie_zone_settings', 'windows_registry_mount_points2', 'windows_registry_bagmru', 'windows_registry_boot_execute', 'windows_registry_timezone', 'windows_registry_service', 'windows_registry_winlogon', 'windows_registry_sam_users', 'olecf_dest_list_entry', 'msie_webcache_container', 'windows_registry_mru_list', 'msie_webcache_containers', 'windows_registry_shutdown', 'windows_registry_usb', 'windows_registry_typedurls', 'windows_registry_mrulistex', 'windows_metadata_deleted_item', 'windows_registry_mstsc_connection', 'windows_registry_mstsc_mru', 'pe_import_import_time'])
```

```
pldfs_srv['task_scheduler_task_cache_entry']['Timestamp_'].iloc[0]
```

Timestamp('2013-08-10 14:48:44.446487')

```
pldfs_srv['task_scheduler_task_cache_entry'][['Timestamp_', 'task_name']].iloc[0:10]
```

	Timestamp_	task_name
0	2013-08-10 14:48:44.446487	Plug and Play Cleanup
1	2013-08-16 14:48:44.477735	Sqm-Tasks
2	2013-08-16 14:48:44.649610	SynchronizeTimeZone
3	2013-08-17 14:48:44.758985	KernelCeipTask
4	2013-08-18 14:48:43.837110	SmartScreenSpecific
5	2013-08-18 14:48:44.743361	AnalyzeSystem
6	2013-08-18 14:48:44.758985	UsbCeip
7	2013-08-19 14:48:44.087110	SQM data sender
8	2013-08-19 14:48:44.149611	SynchronizeTime
9	2013-08-19 14:48:44.321488	Metadata Refresh

```
[113]: xmenu(pldfs_srv)
```

DataFrame visualization menu:

Select DataFrame:

Selected dataframe:

- fs_ntfs_usn_change
- fs_stat
- msie_webcache_container
- msie_webcache_containers
- olecf_dest_list_entry
- olecf_item
- pe_compilation_compilation_time
- pe_import_import_time
- setupapi_log_line
- task_scheduler_task_cache_entry
- windows_distributed_link_tracking_creation
- windows_evtx_record
- windows_lnk_link
- windows_metadata_deleted_item
- windows_registry_bagmru
- windows_registry_boot_execute
- windows_registry_installation
- windows_registry_key_value
- windows_registry_mount_points2

Pandas

- Most used DS library in Python
- Other commonly used are:
 - Numpy
 - SciPy
 - Scikit-Learn
 - Keras
 - Matplotlib

```
df.loc["2020-09-18 05:41:16":"2020-09-18 05:41:18", ["TargetUserSid", "Computer"]]
```

Timestamp	TargetUserSid	Computer
2020-09-18 05:41:16	S-1-5-18	WIN-2IH1TBB9I4Q
2020-09-18 05:41:17	S-1-5-18	WIN-2IH1TBB9I4Q
2020-09-18 05:41:17	S-1-5-96-0-0	WIN-2IH1TBB9I4Q
2020-09-18 05:41:18	S-1-5-20	WIN-2IH1TBB9I4Q
2020-09-18 05:41:18	S-1-5-96-0-1	WIN-2IH1TBB9I4Q

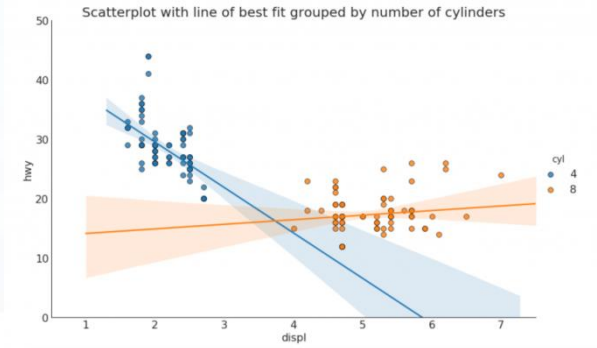
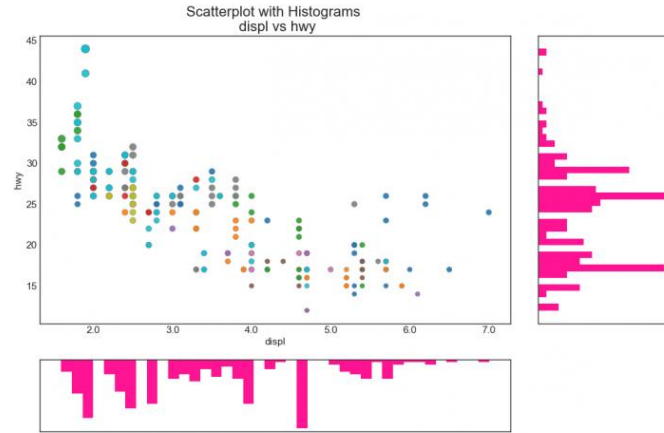
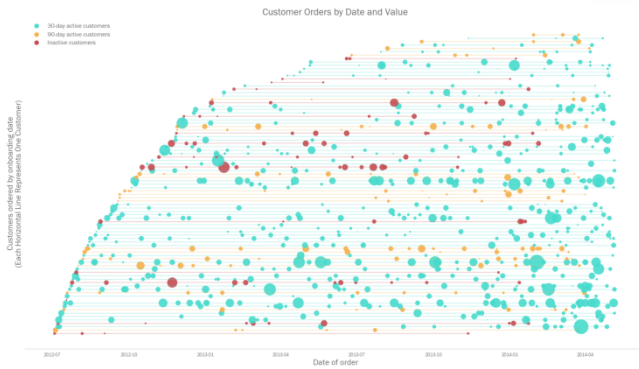
```
df['Computer'].iloc[0]
```

'WIN-2IH1TBB9I4Q'

```
df.query('TargetUserSid == "S-1-5-18").head()
```

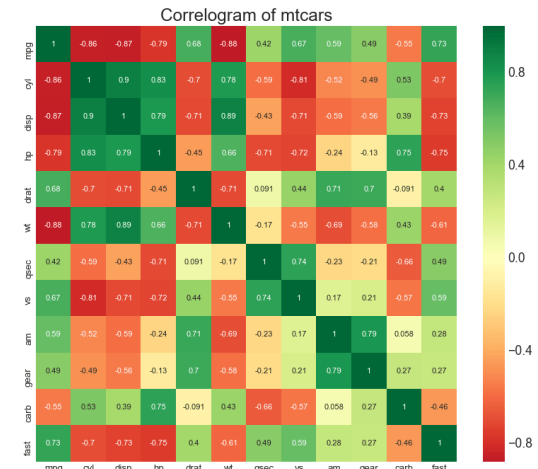
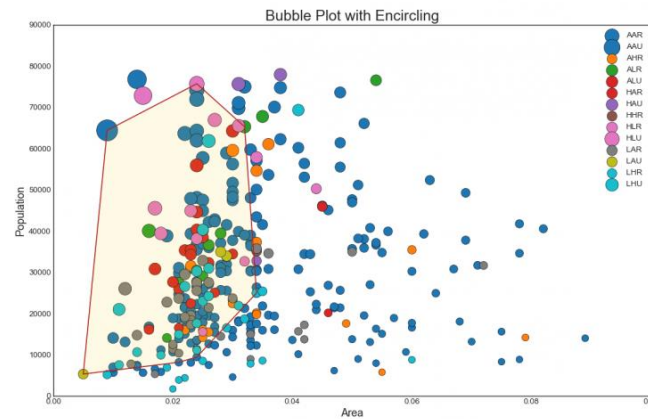
SubjectUserName	SubjectDomainName	SubjectLogonId	TargetUserSid	TargetUserName	TargetDomainName	TargetLogonId	@CorrelationActivityID	LogonType	LogonProcessName
-	-	0x0000000000000000	S-1-5-18	SYSTEM	NT AUTHORITY	0x000000000000003e7	<NA>	0	-
MINWINPC\$	<NA>	0x000000000000003e7	S-1-5-18	SYSTEM	NT AUTHORITY	0x000000000000003e7	{4B73C7C8-8D7E-0001-15CA-734B7E8DD601}	5	Advapi
MINWINPC\$	<NA>	0x000000000000003e7	S-1-5-18	SYSTEM	NT AUTHORITY	0x000000000000003e7	{4B73C7C8-8D7E-0001-15CA-734B7E8DD601}	5	Advapi
MINWINPC\$	<NA>	0x000000000000003e7	S-1-5-18	SYSTEM	NT AUTHORITY	0x000000000000003e7	{4B73C7C8-8D7E-0001-15CA-734B7E8DD601}	5	Advapi
MINWINPC\$	<NA>	0x000000000000003e7	S-1-5-18	SYSTEM	NT AUTHORITY	0x000000000000003e7	{4B73C7C8-8D7E-0001-15CA-734B7E8DD601}	5	Advapi

Matplotlib



Other visualization libraries:

- seaborn
- plotly
- bokeh
- NetworkX
- altair



DS4N6. The Road So Far

DS4N6



CHRYSALIS

D4ML

HAM

**ADversAry
eMulator**

DAISY VM

CHRYSALIS

Function	Usage	Type	Description
whatis()	whatis(obj)	CLI	Identifies the forensic data type of an object (DataFrame -df- or DataFrame Collection -dfs-)
xread()	xread(options)	GUI	Reads tool output data (e.g. plaso output) and stores it in a df/dfs
xmenu()	xmenu(obj)	GUI	Used to easily select a dataframe from dfs, or a column from a df, displaying the selected data and allowing manual (Excel-like) analysis on it
xanalysis()	xanalysis(obj, options)	GUI	Displays a menu with the advanced analysis functions available for the data type (i.e. forensic artifact) given
xdisplay()	xdisplay()	GUI	Used to select the display settings for the dataframes that will be displayed (max. rows, max. columns, etc.)
simple()	df.simple(options)	CLI	Simplifies forensic output (df) showing only the most interesting columns for analysis.
xgrep()	xgrep(obj, options)	CLI	UNIX-like grep for the DataFrame world. Allows the user to search for a regular expression in a DF column or full DF

For more information, visit <https://www.ds4n6.io/tools/chrysalis.html>

DAISY

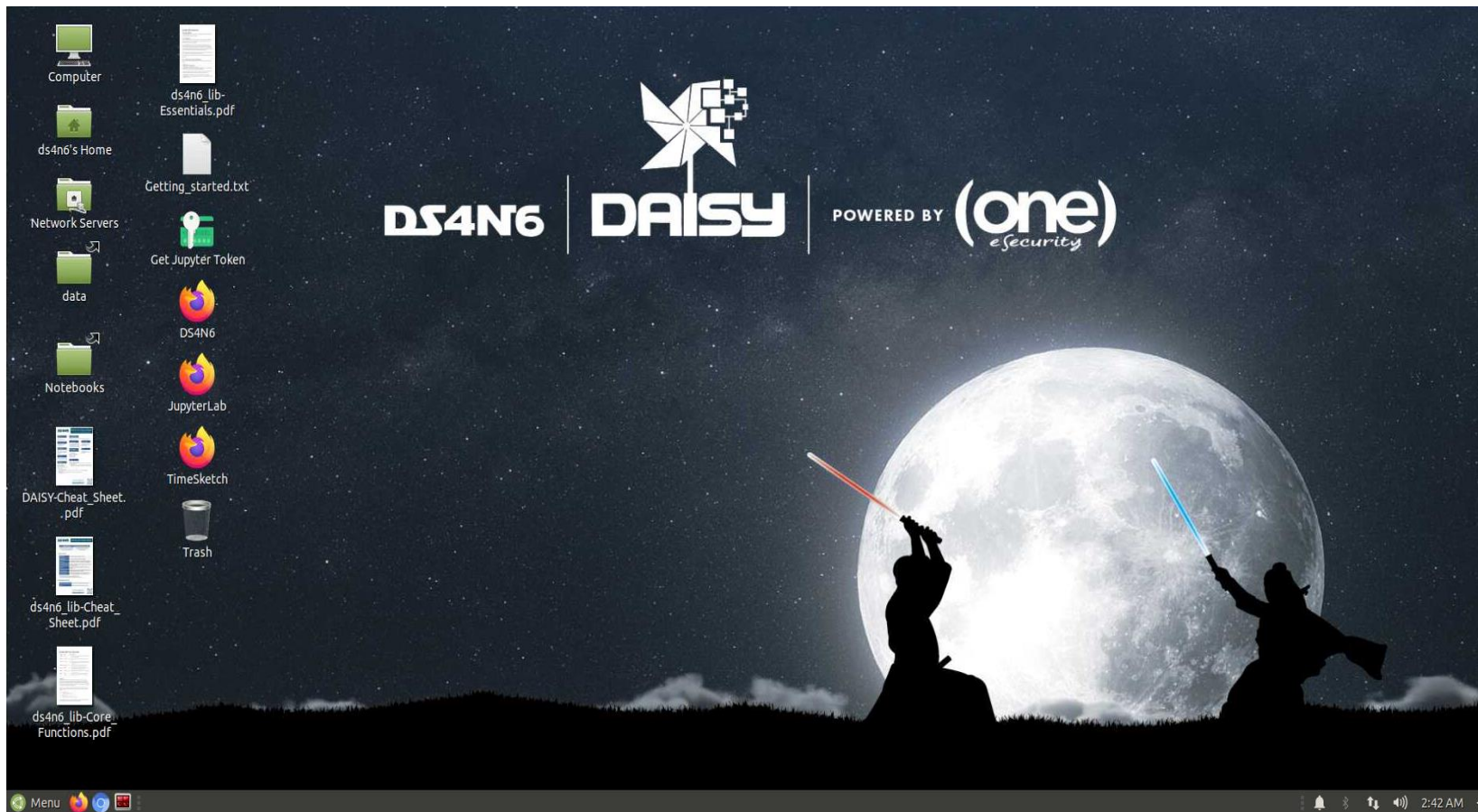


DFIR	
Data	D
Artificial	A
Intelligence	I
Science	S
	Y



www.ds4n6.io/daisy

DS4N6



The Case: The Stolen Szechuan Sauce



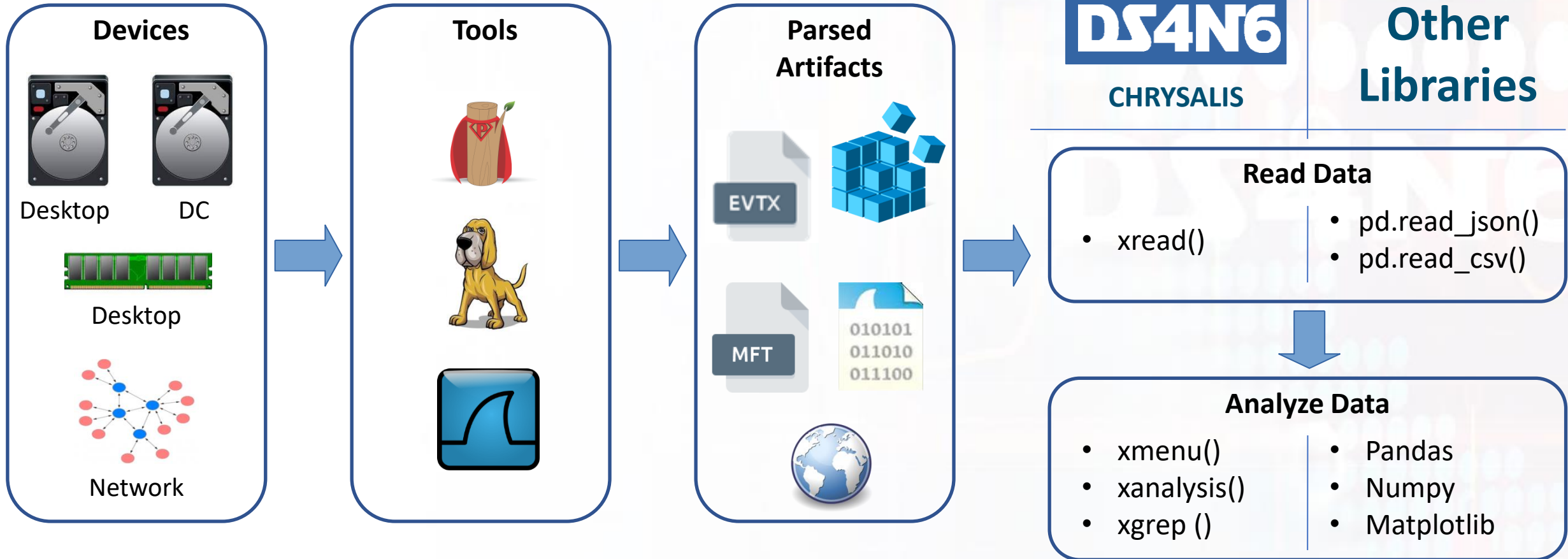
Read the whole case here:
<https://dfirmadness.com/the-stolen-szechuan-sauce/>

- The FBI contacts us: our secret Szechuan Sauce recipe is on the Dark Web
- The recipe was on the Domain Controller. There are more interesting files in the share
- We receive the Domain Controller disk, an affected desktop computer disk and memory and a pcap with the network traffic of the attack date
- The computers were in Colorado (UTC -6)



**We need to find out WHO,
WHEN and HOW did it!**

The Case: The Stolen Szechuan Sauce Case





All the details about this Workshop:
ds4n6.io/odscwest21

HANDS
ON



DS4N6

 ds4n6.io

 [@ds4n6_io](https://twitter.com/ds4n6_io)

 [DS4N6](https://www.youtube.com/DS4N6)

(one) eSecurity

 [one-esecurity.com](https://www.one-esecurity.com)

 [One_eSecurity](https://twitter.com/One_eSecurity)