Run a DFIR investigation the easy way: Revealer Toolkit 2

Abraham Pasamar
Juan Vera

Something about the speakers

Abraham Pasamar

Juan Vera

Something about our company

- 15 years of experience in cybersecurity
- Incident Response
- Forensic Lab
- Red Teams

Lessons learned during these years:

- All cases are different…
- and yet, all cases have **similar procedures**
- **Automated procedures** are key to success
- To handle multiple cases and multiple analysts we need to enforce **work organization**

/Rootəd

DFIR Analysis tools

DFIR analysis tools

- Commercial solutions: EnCase, FTK, OSForensics.
- Nirsoft
- Autopsy
- Kuiper
- ...

NirSoft

EnCase

Kuiper

FTK

FORENSIC TOOLKIT

/Rooted

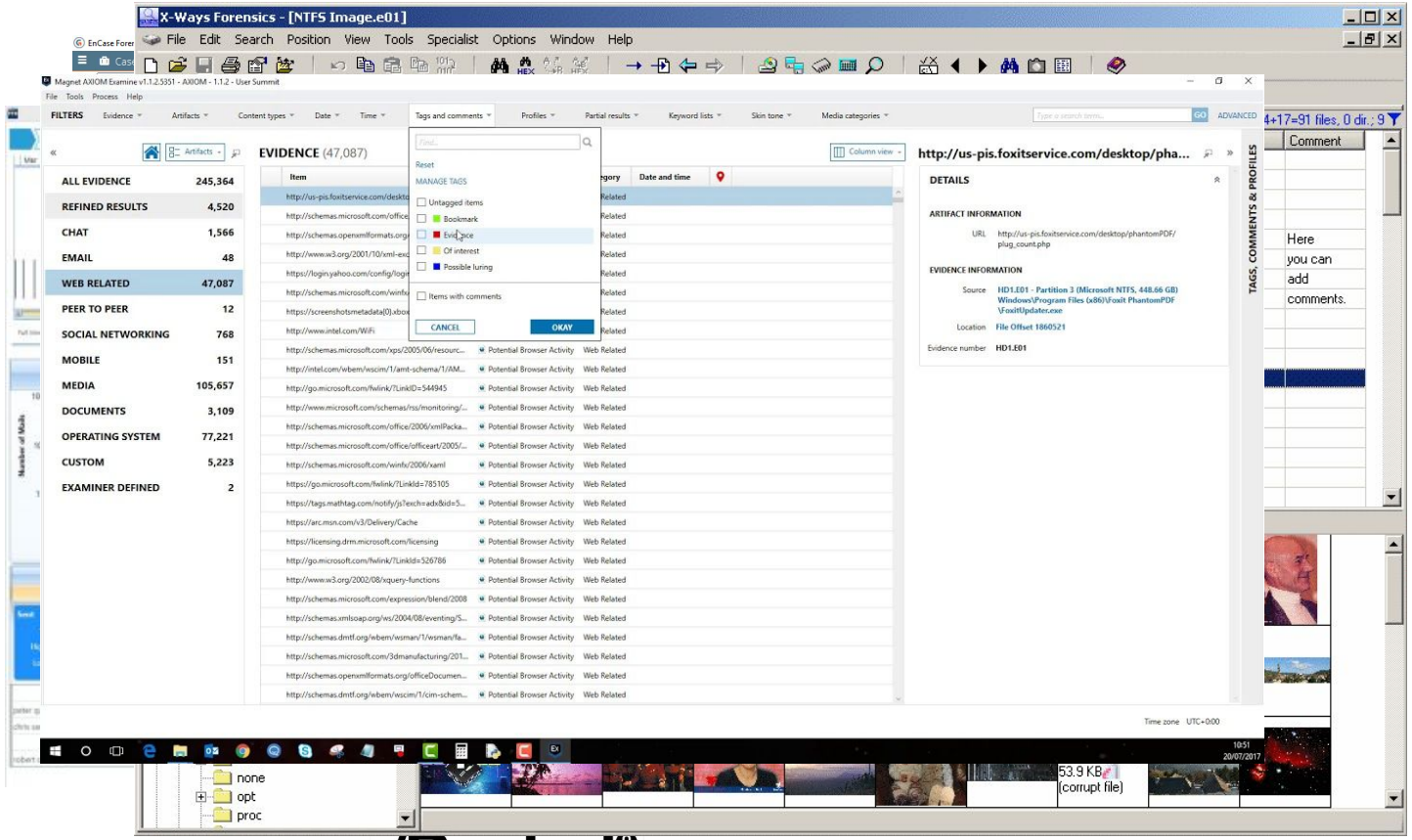
Commercial solutions

Encase

FTK

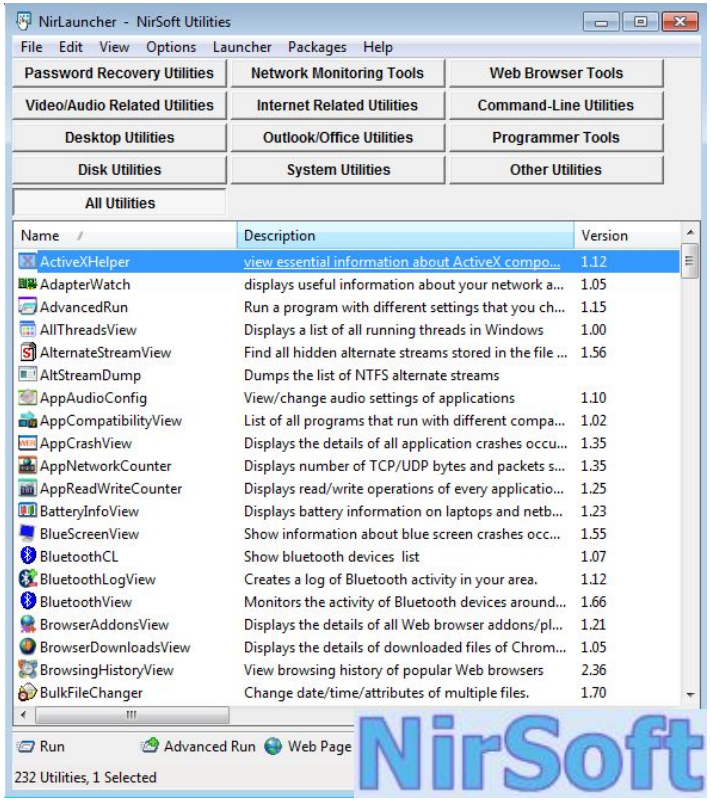
X-WAYS

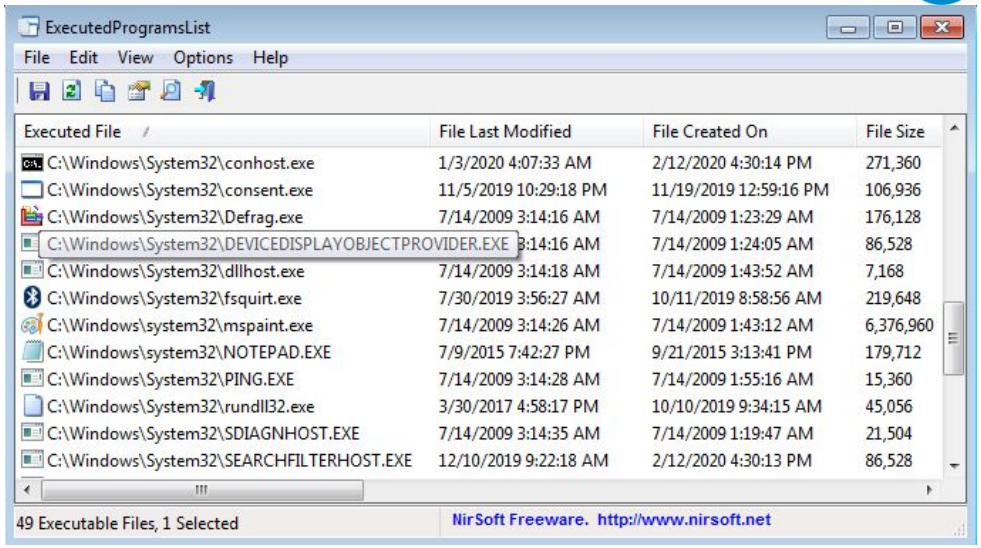
OTHERS

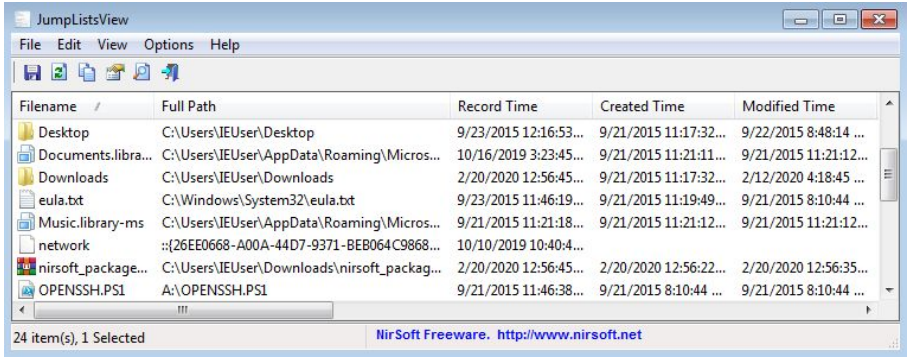


/Rooted

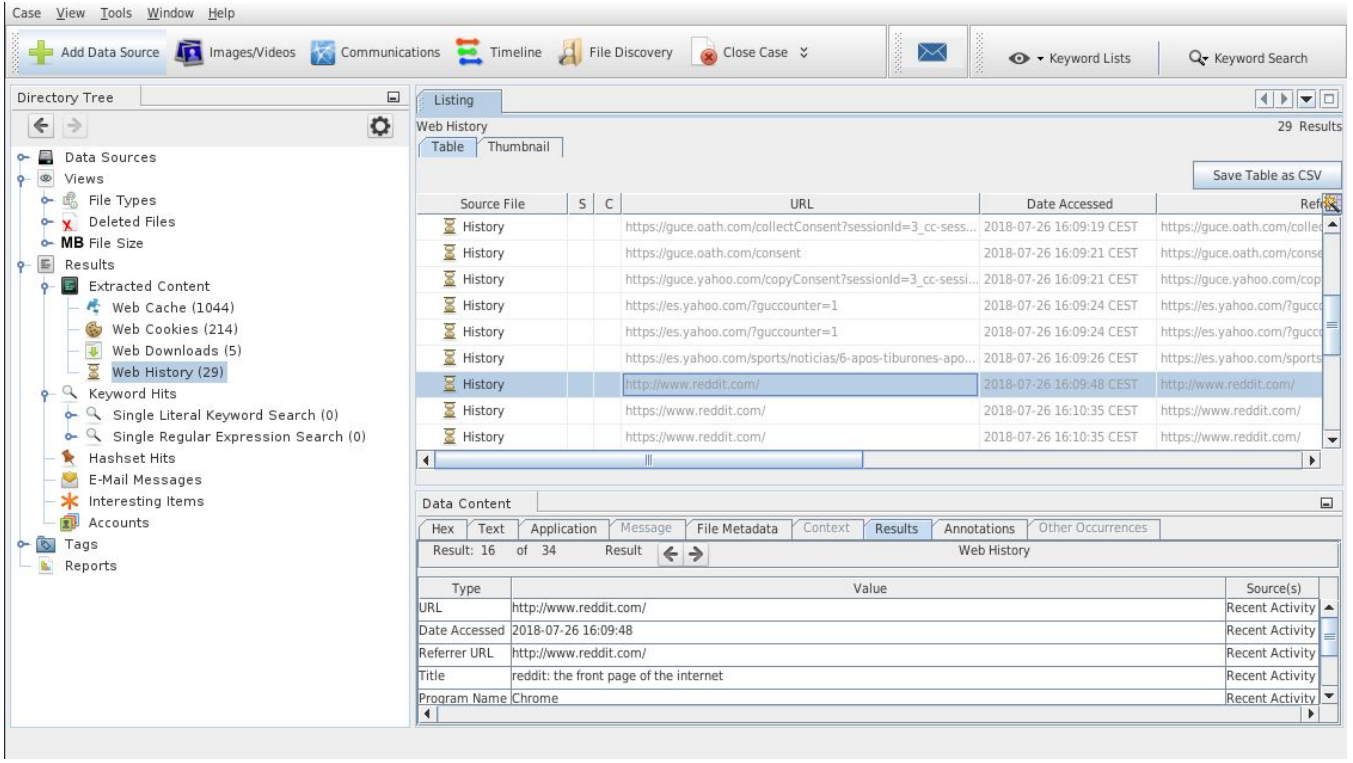
NirSoft


NirLauncher - NirSoft Utilities
File Edit View Options Launcher Packages Help
Password Recovery Utilities
Network Monitoring Tools
Web Browser Tools
Video/Audio Related Utilities
Internet Related Utilities
Command-Line Utilities
Desktop Utilities
Outlook/Office Utilities
Programmer Tools
Disk Utilities
System Utilities
Other Utilities
All Utilities
Name
Description
Version
ActiveXHelper
view essential information about ActiveX compo...
1.12
AdapterWatch
displays useful information about your network a...
1.05
AdvancedRun
Run a program with different settings that you ch...
1.15
AllThreadsView
Displays a list of all running threads in Windows
1.00
AlternateStreamView
Find all hidden alternate streams stored in the file ...
1.56
AltStreamDump
Dumps the list of NTFS alternate streams
AppAudioConfig
View/change audio settings of applications
1.10
AppCompatibilityView
List of all programs that run with different compa...
1.02
AppCrashView
Displays the details of all application crashes occu...
1.35
AppNetworkCounter
Displays number of TCP/UDP bytes and packets s...
1.35
AppReadWriteCounter
Displays read/write operations of every applicatio...
1.25
BatteryInfoView
Displays battery information on laptops and netb...
1.23
BlueScreenView
Show information about blue screen crashes occ...
1.55
BluetoothCL
Show bluetooth devices list
1.07
BluetoothLogView
Creates a log of Bluetooth activity in your area.
1.12
BluetoothView
Monitors the activity of Bluetooth devices around...
1.66
BrowserAddonsView
Displays the details of all Web browser addons/pl...
1.21
BrowserDownloadsView
Displays the details of downloaded files of Chrom...
1.05
BrowsingHistoryView
View browsing history of popular Web browsers
2.36
BulkFileChanger
Change date/time/attributes of multiple files.
1.70
Run
Advanced Run
Web Page
232 Utilities, 1 Selected
NirSoft

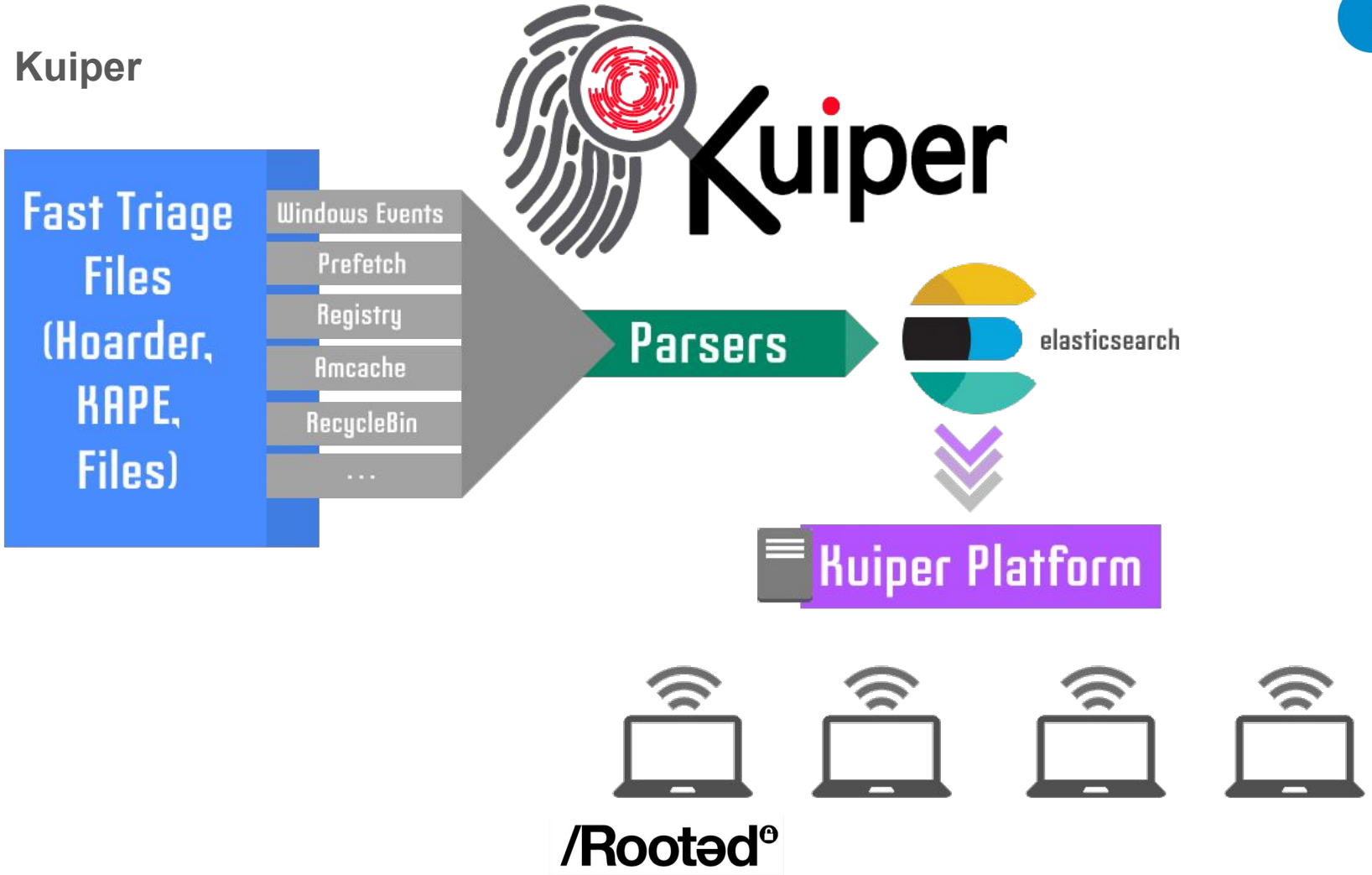

ExecutedProgramsList
File Edit View Options Help
Executed File
File Last Modified
File Created On
File Size
C:\Windows\System32\conhost.exe
1/3/2020 4:07:33 AM
2/12/2020 4:30:14 PM
271,360
C:\Windows\System32\consent.exe
11/5/2019 10:29:18 PM
11/19/2019 12:59:16 PM
106,936
C:\Windows\System32\Defrag.exe
7/14/2009 3:14:16 AM
7/14/2009 1:23:29 AM
176,128
C:\Windows\System32\DEVICEDISPLAYOBJECTPROVIDER.EXE
7/14/2009 1:24:05 AM
86,528
C:\Windows\System32\dllhost.exe
7/14/2009 3:14:18 AM
7/14/2009 1:43:52 AM
7,168
C:\Windows\System32\fsquirt.exe
7/30/2019 3:56:27 AM
10/11/2019 8:58:56 AM
219,648
C:\Windows\system32\mspaint.exe
7/14/2009 3:14:26 AM
7/14/2009 1:43:12 AM
6,376,960
C:\Windows\system32\NOTEPAD.EXE
7/9/2015 7:42:27 PM
9/21/2015 3:13:41 PM
179,712
C:\Windows\System32\PING.EXE
7/14/2009 3:14:28 AM
7/14/2009 1:55:16 AM
15,360
C:\Windows\System32\rundll32.exe
3/30/2017 4:58:17 PM
10/10/2019 9:34:15 AM
45,056
C:\Windows\System32\SDIAGNHOST.EXE
7/14/2009 3:14:35 AM
7/14/2009 1:19:47 AM
21,504
C:\Windows\System32\SEARCHFILTERHOST.EXE
12/10/2019 9:22:18 AM
2/12/2020 4:30:13 PM
86,528
49 Executable Files, 1 Selected
NirSoft Freeware. http://www.nirsoft.net


JumpListsView
File Edit View Options Help
Filename
Full Path
Record Time
Created Time
Modified Time
Desktop
C:\Users\IEUser\Desktop
9/23/2015 12:16:53...
9/21/2015 11:17:32...
9/22/2015 8:48:14 ...
Documents.libra...
C:\Users\IEUser\AppData\Roaming\Micros...
10/16/2019 3:23:45...
9/21/2015 11:21:11...
9/21/2015 11:21:12...
Downloads
C:\Users\IEUser\Downloads
2/20/2020 12:56:45...
9/21/2015 11:17:32...
2/12/2020 4:18:45 ...
eula.txt
C:\Windows\System32\eula.txt
9/23/2015 11:46:19...
9/21/2015 11:19:49...
9/21/2015 8:10:44 ...
Music.library-ms
C:\Users\IEUser\AppData\Roaming\Micros...
9/21/2015 11:21:18...
9/21/2015 11:21:12...
9/21/2015 11:21:12...
network
::{26EE0668-A00A-44D7-9371-BEB064C9868...
10/10/2019 10:40:4...
nirsoft_package...
C:\Users\IEUser\Downloads\nirsoft_packag...
2/20/2020 12:56:45...
2/20/2020 12:56:22...
2/20/2020 12:56:35...
OPENSSH.PS1
A:\OPENSSH.PS1
9/21/2015 11:46:38...
9/21/2015 8:10:44 ...
9/21/2015 8:10:44 ...
24 item(s), 1 Selected
NirSoft Freeware. http://www.nirsoft.net

Autopsy


Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
File Discovery
Close Case
Keyword Lists
Keyword Search
Directory Tree
Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
Web Cache (1044)
Web Cookies (214)
Web Downloads (5)
Web History (29)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Web History
29 Results
Table
Thumbnail
Save Table as CSV
Source File
S
C
URL
Date Accessed
History https://guce.oath.com/collectConsent?sessionId=3_cc-sess... 2018-07-26 16:09:19 CEST
History https://guce.oath.com/consent 2018-07-26 16:09:21 CEST
History https://guce.yahoo.com/copyConsent?sessionId=3_cc-sessi... 2018-07-26 16:09:21 CEST
History https://es.yahoo.com/?guccounter=1 2018-07-26 16:09:24 CEST
History https://es.yahoo.com/?guccounter=1 2018-07-26 16:09:24 CEST
History https://es.yahoo.com/sports/noticias/6-apos-tiburones-apo... 2018-07-26 16:09:26 CEST
History http://www.reddit.com/ 2018-07-26 16:09:48 CEST
History https://www.reddit.com/ 2018-07-26 16:10:35 CEST
History https://www.reddit.com/ 2018-07-26 16:10:35 CEST
Data Content
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
Result: 16 of 34 Result
Web History
Type
Value
Source(s)
URL http://www.reddit.com/ Recent Activity
Date Accessed 2018-07-26 16:09:48 Recent Activity
Referrer URL http://www.reddit.com/ Recent Activity
Title reddit: the front page of the internet Recent Activity
Program Name Chrome Recent Activity

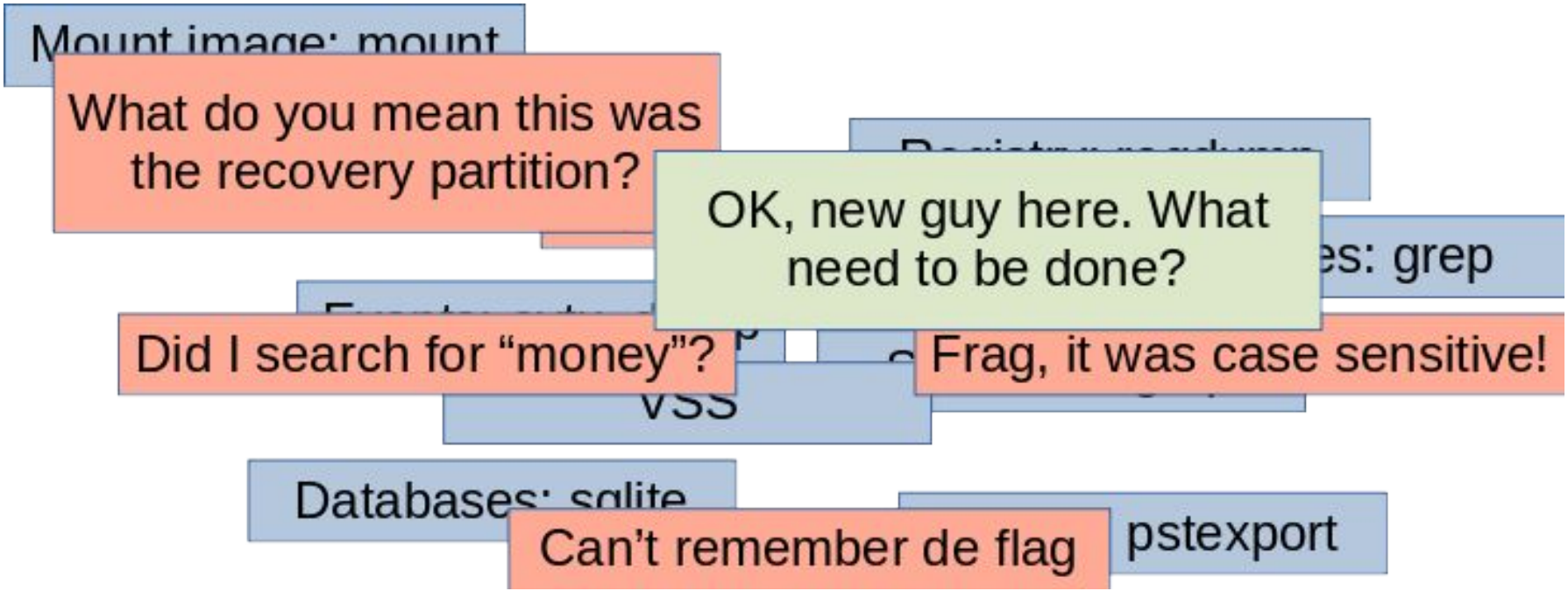
Kuiper


Kuiper
Fast Triage Files (Hoarder, KAPE, Files)
Windows Events
Prefetch
Registry
Amcache
RecycleBin
...
Parsers
elasticsearch
Kuiper Platform
/Rooted

DFIR Open Source Tools

- Sleuthkit
- Tika
- ElasticSearch
- Kibana
- Regripper
- Radare2
- Yara
- Hindsight
- Apollo Project
- Srum-dump
- Spotlight_parser
- Volatility

A typical investigation using OS tools



The Revealer Toolkit 2

- Give back to the world!
- Give control about the output to the analyst
- Open source
- Chains of modules
- Automate repetitive tasks
- Prevent human errors
- Run common tasks for all cases

Overview

The RVT2 is…

- A set of predefined chains of commands to run on forensic images
- A converter between “anything” to JSON
- An interface to many OS tools: PSTParser, RegRipper, ag, SQLite, ElasticSearch…
- A way to structure the output from the tools
- A logger for the already run commands

IF THE TOOL DOES THE HARD WORK, THE ANALYST HAS LONGER TIME TO THINK ABOUT THE CASE

Strong points

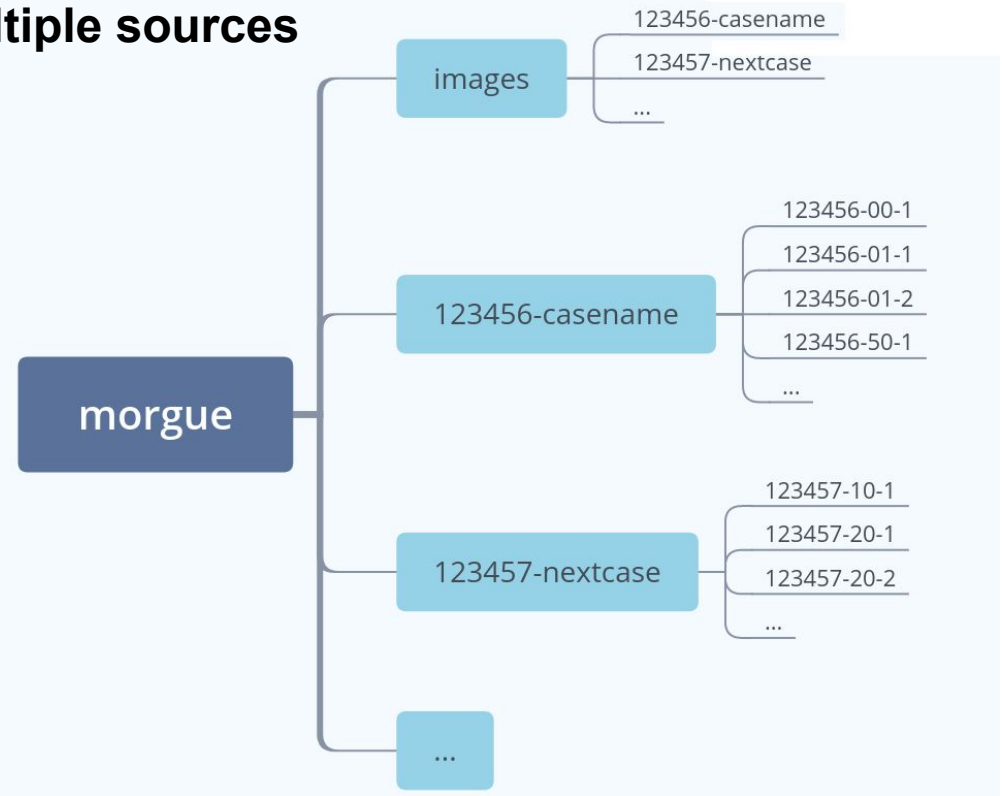
- **Text output: chainable with other commands**
- **Automation of routine tasks: let the analyst think**
- **Organized and reproducible output: the case can be easily transferred to other analysts**
- **Python: extensible**
- **All actions are registered: reports, monitoring, statistics...**
- **Tested for years and hundreds of cases**
- **Joint work of dozens of developers**

History and developers

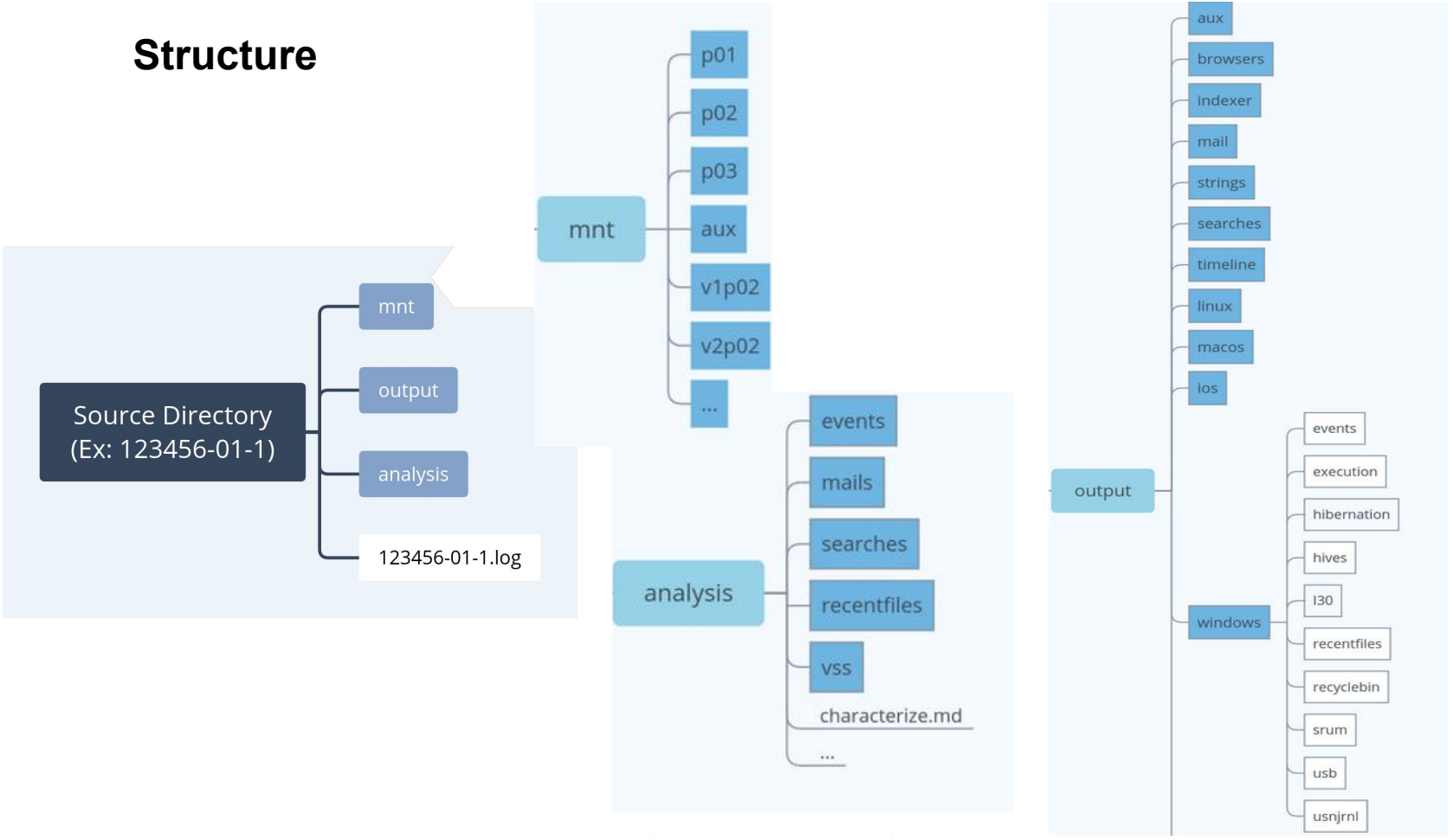
- Manel Ginés, alias xkulio, started the project in Bash/Perl as *Chanchullos-revealer*.
- Luís Gómez, alias Pope
- Jose Navarro, first commit in Google Code in 2008
- Sara Rincón
- Jose Selvi
- Abraham Pasamar
- Manel Cardona, first version in Python.
- Carlos Férnandez
- Imanol Barba
- Eduard Sanou
- Arnau Estevanell
- Neus Boix
- Pau García

Modules and Jobs

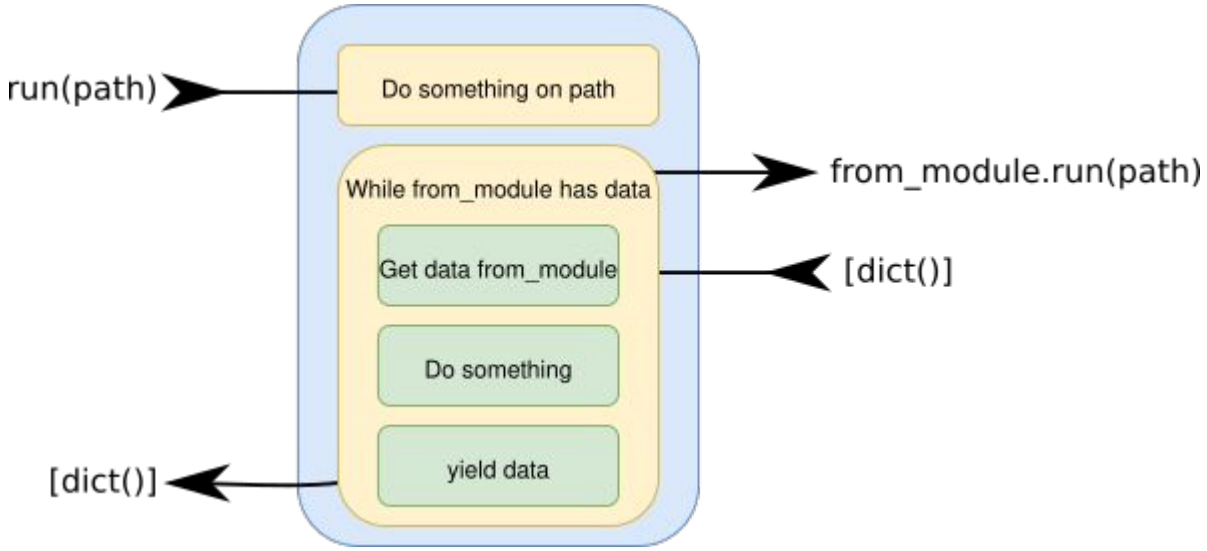
Handling multiple sources



Structure

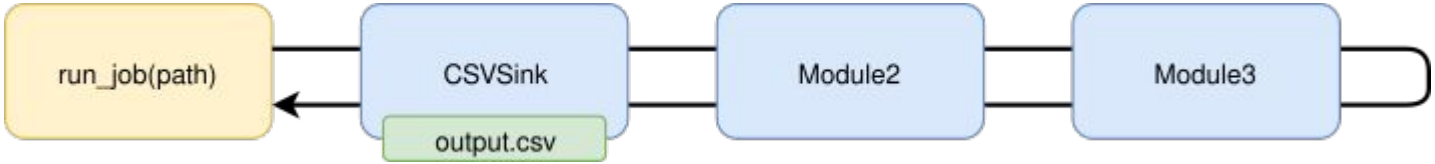


Modules



A **module** is a class that extends base.job.BaseModule. A module does something very specific, such as reading a CSV, writing a JSON file or parsing an EVTX file suing an external tool. A module takes a path as an input, reads its configuration and yields a dictionary. That is to say: a module returns a generator of dictionaries.

Jobs



A **single job** is a chain of modules connected one after the other to perform a complex task. For example, read the contents of a CSV file, filter out the lines not containing a regex, save the results to a JSON file, convert the JSON file to be ready to be sent to ElasticSearch... A chain can have any number of modules, or even just one since a module can run as a single job. The modules in a single job are chained together, and share information to each other.

Job example: preforensics

```
[windows.preforensics]
help_section: windows
jobs:
      mount
      allocfiles vss={vss}
      fs_timeline vss={vss}
      windows.autorip vss={vss}
      windows.characterize
      windows.hives vss={vss}
      windows.recentfiles vss={vss}
      windows.evtx_export vss={vss}
      windows.evtx vss={vss}
      windows.events
      windows.exec vss={vss}
      windows.activity_cache vss={vss}
      windows.usb vss={vss}
      windows.recycle vss={vss}
      windows.usnjrnl vss={vss}
      ; windows.bits vss={vss}
      browsers vss={vss}
      windows.srum vss={vss}
```

Common

- **mount**: Mount all partitions of a disk image.
- **umount**: Unmount all partitions of a disk image
- **fs_timeline**: Generate a timeline of a filesystem according to MFT.
- **allocfiles**: Generate allocated files in a disk image
- **characterize:** Describes basic information about disk and partitions.
- **strings**: Extract all strings of printable characters (ascii and unicode) from disk data.
- **search_strings**: Search defined keywords in disk strings. The list of keywords must be defined in a separated file, including the keyword name and a regex if desired.
- **search_email**: Search emails patterns in strings
- **search_accounts**: Search account patterns in strings
- **search_output**: Search regular expressions in a source output directories, except for strings, searches and parser folders.
- **browsers**: Extract information about most common internet browsers (chrome, firefox, safari, edge).
- **skype**: Extract contacts, messages, calls from Skype databases

Windows

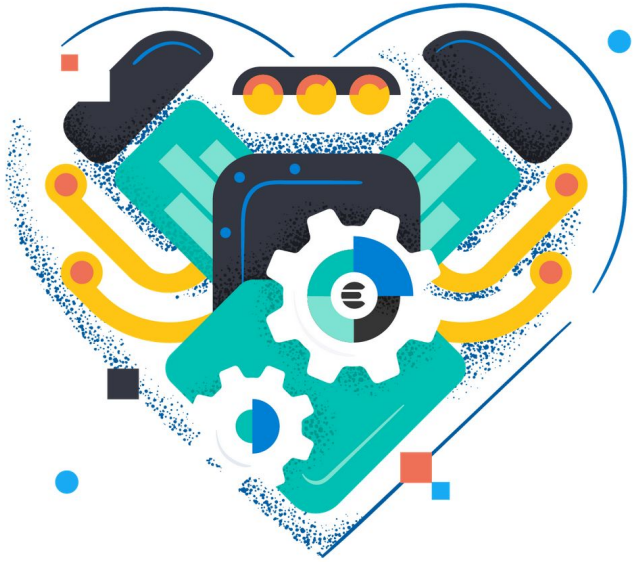
- **windows.preforensics:** Main set of forensic analysis jobs to run on a Windows disk partition
- **windows.characterize**: Describes basic information about disk and Windows partitions.
- **windows.recentfiles**: Parse lnk and jumplist files from a Windows image. Generates a summary file with all recent files sources.
- **windows.events:** Parse Windows event files to get relevant logs events.
- **windows.exec**: Extract and parse Windows artifacts related with applications execution (Prefetch, RFC, BAM).
- **windows.autorip**: Extracts an extensive set of keys from Windows Registry hives. Results are organized according to its information type.
- **windows.recycle**: Parse files in (or deleted from) Windows Recycle Bin
- **windows.srum**: Extract and parse SRUM (System Resource Utilization Monitor) from a windows OS
- **windows.usnjrnl**: Parse NTFS UsnJrnl
- **windows.hiberfil**: Decompress hiberfil.sys and extract some artifacts
- **windows.bits**: Parse Background Intelligent Transfer Service (BITS)
- **windows.activity_cache**: Parse ActivitiesCache database
- **windows.i30**: Parse I30 files to obtain a timeline

ios

- **ios.preforensics**: Run a selected set of jobs in this module: unback, characterize, databases, cookies, whatsapp
- **ios.apollo**: Parse iOS databases from the APOLLO project (https://github.com/mac4n6/APOLLO).
- **ios.databases**: Parse iOS databases not in the APOLLO project
- **ios.timeline**: Parse manifest file and generate a body and a timeline csv using mactime
- **ios.cookies**: Parse cookies in /HomeDomain/Library/Cookies
- **ios.whatsapp**: Parse WhatsApp database
- **ios.avere_whatsapp**: Avere WhastApp messages in IOS

Indexer

- **indexer.directory**: Parse a directory.
- **indexer.save**: Save a previously indexed database in an ElasticSearch server. Alternative to `elasticdump`.
- **indexer.index_timeline_body**: Index a BODY file provided in the path.
- **indexer.mails**: Export, parse and characterize contents of every pst or ost file found in a source
- **indexer.blind_searches**: Blind searches on a parsed JSON file, result from **indexer.save**.
- **indexer.query_and_tag**: Query elastic, select all related documents (containers, attachments..) and tag all of them. You must indexer.save the output
- **indexer.export**: Query elastic, select all documents matching a query and export them to a JSON.
- **indexer.mails**: Export, parse and characterize contents of every pst or ost file found in a source



Job `indexer.directory`

Parse a directory and save in `/morgue/mycase/mysource/output/indexer/mysource.json`. This file is compatible with indexers.

Configurable parameters

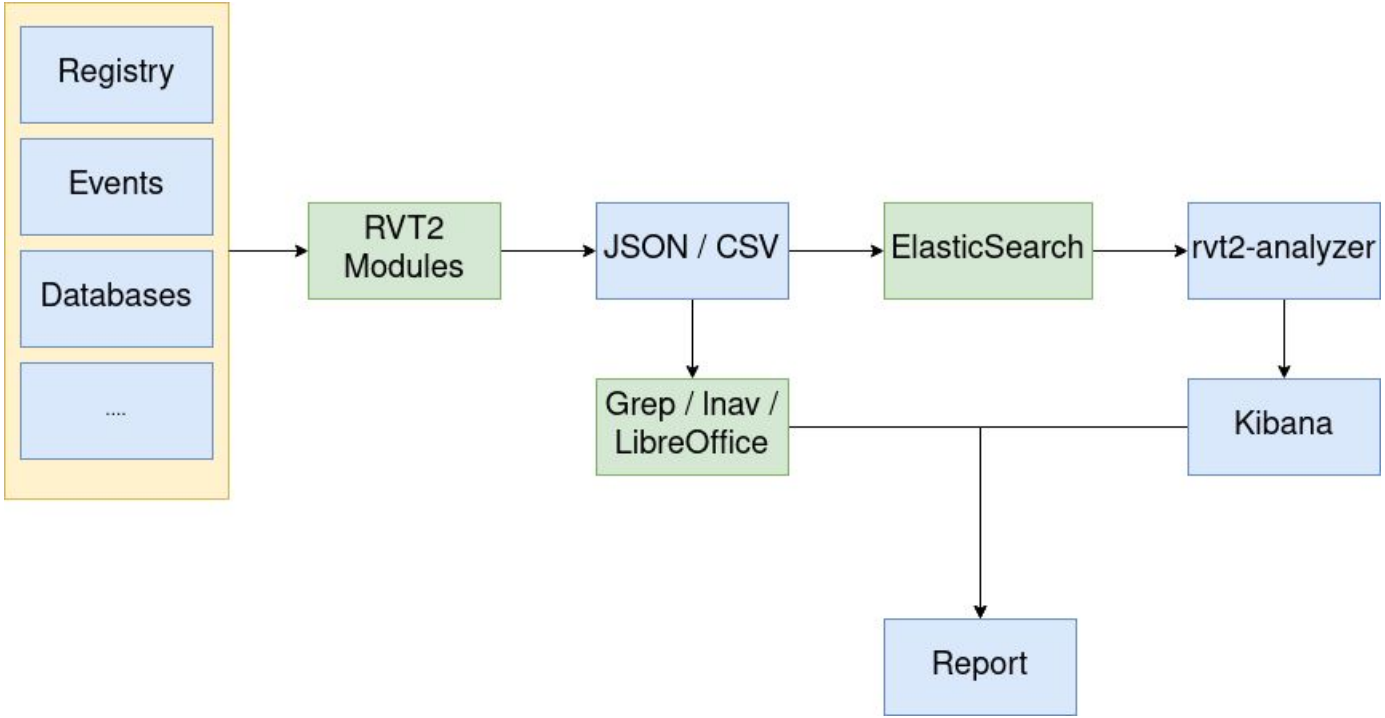
- path: The path to the directory to parse | **Default:** ``
- outfile: Save the result of the parsing in this file | **Default:** `/morgue/mycase/mysource/output/indexer/mysource.json`
- name: The name of the indice to save the parsed files | **Default:** `mysource`
- rvtindex: The name of the indice to save metadata. Set to empty to not save metadata. | **Default:** `rvtindexer`
- restartable: If True, parsing can be restarted from the last error. Use with care! | **Default:** `False`
- filter: List of file categories to parse. If not provided, parse all files. Predefined categories can be found in "file_categories.cfg" configuration file | **Default:** ``

Context

- morgue: `/morgue`
- casedir: `/morgue/mycase`
- casename: `mycase`
- source: `mysource`
- modules:
  ```
  base.output.JSONSink outfile='{outfile}' file_exists=APPEND
  indexer.elastic.ElasticSearchAdapter description="mysource" rvtindex="{rvtindex}" name="{name}"
  base.mutations.DateFields
  base.directory.DirectoryFilter restartable={restartable} filter='{filter}'
  base.directory.FileClassifier check_extension=False
  indexer.tikaparser.TikaParser
  ```
- outfile: `/morgue/mycase/mysource/output/indexer/mysource.json`
- path: `/morgue/mycase/mysource/mnt`

RVT2 Ecosystem

Rvt2 process

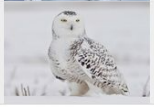


Rvt2: Console interface

rvt2 --morgue morgue --casename 112233-test -j status

rvt2 --morgue morgue --casename 112233-test --source 1-indexer -j indexer.directory -p

Rvt2-analyzer: web interface

combo(28)	9.118456	***content***: (),this.editMenu.close(),this.appContext.getView("*feather*-aviary-view f.fire("subviewViewEvent","make in view",n),e.use("*feather*-aviary-view	Tags	
combo(28)	9.118456	***content***: (),this.editMenu.close(),this.appContext.getView("*feather*-aviary-view f.fire("subviewViewEvent","make in view",n),e.use("*feather*-aviary-view	Tags	
/embedded-1 (inside *Bibliography - Snowy Owl 14 April 2014 - GLOW posting.xls*)	9.331031	***path***: /p06/Users/Sarah M/Downloads/Bibliography - Snowy *Owl* ***filename***: Bibliography - Snowy *Owl* 14 April 2014 - GLOW posting.xls	Tags	
Great Horned Owl Info.lnk	9.331031	***path***: AppData/Roaming/Microsoft/Windows/Recent/Great Horned *Owl* ***filename***: Great Horned *Owl* Info.lnk	Tags	
Snowy Owl Care.lnk	10.073285	***path***: M/AppData/Roaming/Microsoft/Windows/Recent/Snowy *Owl* ***filename***: Snowy *Owl* Care.lnk	Tags	
Snowy Owl 3.jpg	10.154173		Tags	
Snowy Owl 4.jpg	10.154173		Tags	
Snowy Owl 2.jpg	10.154173		Seen	
/Emails.xml (inside *Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags	
/Emails.xml (inside *87acc1f3ad80d20125000000181f581f.Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags	
/Emails.xml (inside *Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags	
what is this.html	12.118093	***content***: Tags Beta animal *bird*	Tags	

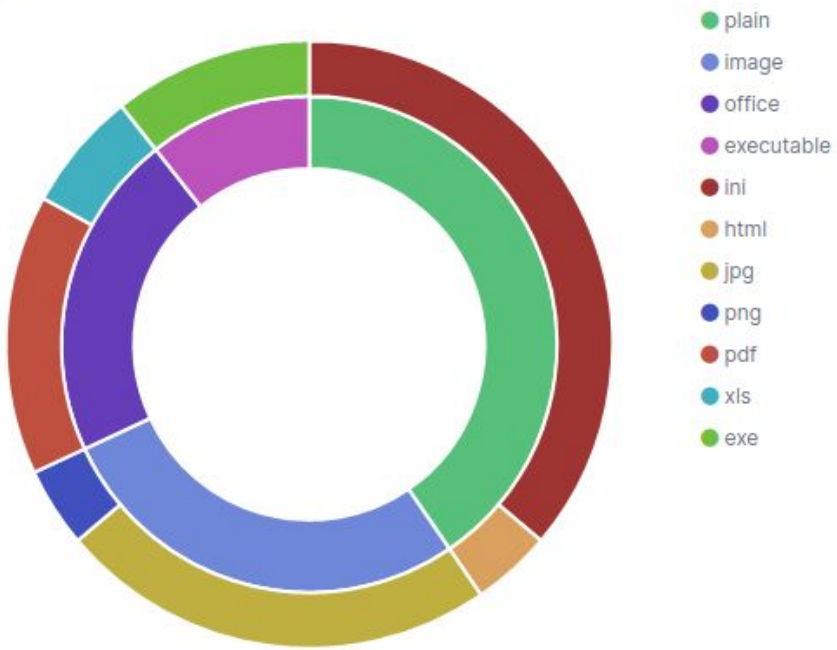
Rvt2-analyzer: Kibana dashboards

Files Count

Directories	Count
100100-07-1/mnt/p06/Users/Sarah M/Downloads	48
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care	24
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets	16
100100-07-1/mnt/p06/Users/Sarah M/Desktop	12
100100-07-1/mnt/p06/Users/Sarah M/Desktop/WOLf Awsome_files	12
100100-07-1/mnt/p06/Users/Sarah M/Desktop/what is this_files	12
100100-07-1/mnt/p06/Users/Sarah M/Documents	8
100100-07-1/mnt/p06/Users/Sarah M	4
100100-07-1/mnt/p06/Users/Sarah M/Contacts	4
100100-07-1/mnt/p06/Users/Sarah M/Favorites	4

Export: Raw Formatted

File Type



Example:
Digital Corpora - Owl

2018 OWL (*Digital Corpora*)

In a jurisdiction where Owls are illegal to trade and buy, two users are discussing the illegal trade of owls. The computer and mobile device taken into evidence are of a user who is attempting to purchase owls illegally. The user has contacted another user who can provide an owl in exchange for cash. An owl is decided upon, and an exchange is scheduled.

https://digitalcorpora.org/corpora/scenarios/2018-owl

Sources:

- PC Windows
- Nexus Android

Incident simulation - Questions solution

These questions are based on "the five W":

WHAT?

WHEN?

WHERE?

WHO?

WHY?

and bonus...HOW?

Source Characterization

```
$ sudo rvt2 --source
100100-07-1 -j mount

$ rvt2 --source 100100-07-1 -j
windows.characterize
```

OS Information

- ProductName: Windows 10 Pro
- ComputerName: = DESKTOP-KLOQJ0V
- ProductId: 00330-50295-68670-AAOEM
- RegisteredOwner: Sarah McAvoy
- RegisteredOrganization: Hewlett-Packard Company
- CurrentVersion: 6.3
- CurrentBuild: 14393
- InstallationType: Client
- EditionID: Professional
- ProcessorArchitecture: AMD64
- TimeZone: Eastern Standard Time (5 hours)
- InstallDate: Fri Jan 27 02:58:47 2017 (UTC)
- ShutdownTime: Mon Jan 30 22:46:43 2017 (UTC)

Users

User	Creation date	Last login/logoff
Administrator [500]	27-01-2017 02:14:33 UTC	27-01-2017 02:06:52 UTC
Guest [501]	27-01-2017 02:14:33 UTC	Never
DefaultAccount [503]	27-01-2017 02:14:33 UTC	Never
Sarah McAvoy [1001]	26-01-2017 23:41:56 UTC	27-01-2017 01:48:12 UTC
Sarah M [1002]	27-01-2017 00:33:10 UTC	02-02-2017 21:24:14 UTC

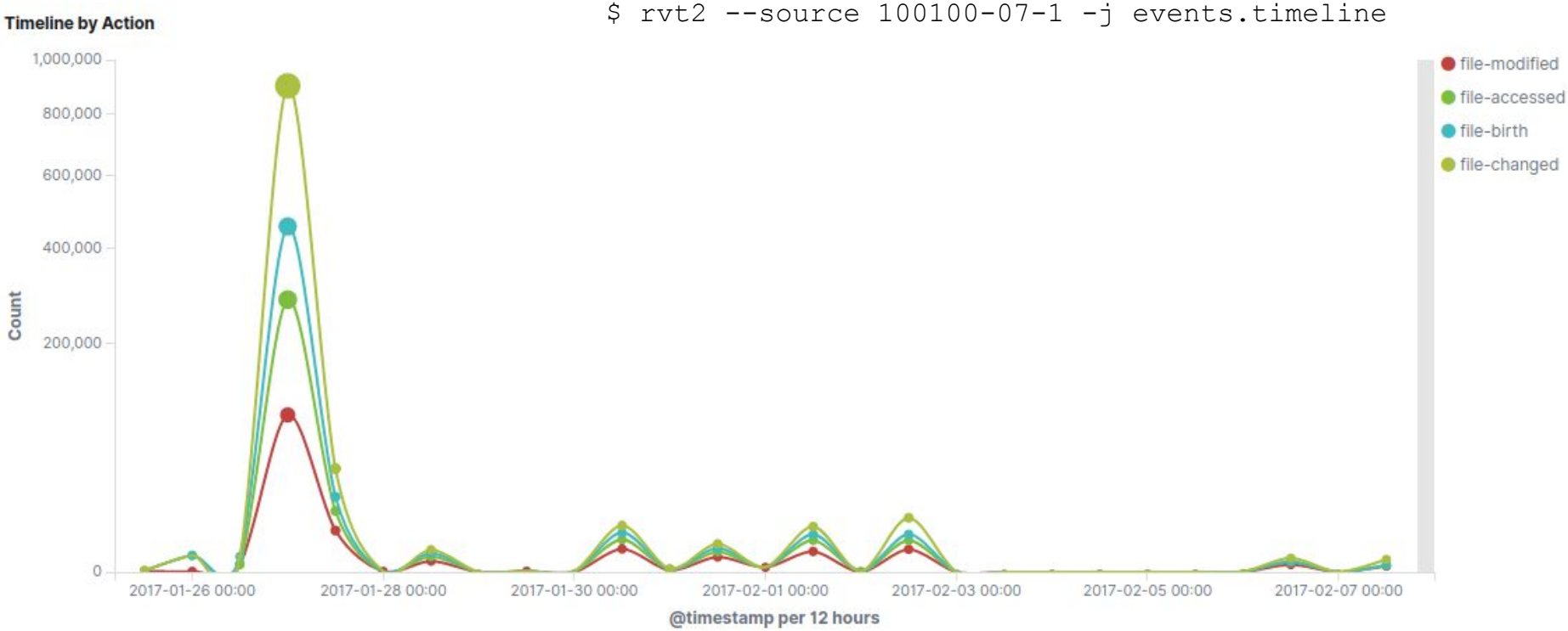
File Analysis

```
$ rvt2 --source 100100-07-1 -j allocfiles
```

```
$ grep -i owl 100100-07-1/output/auxdir/alloc_files.txt
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 2.jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 3.jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 4.jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl.jpg
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Owl_Emergency_Care.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Owl_Keeping.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy Owl Care.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy_Owl.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/Owl_Keeping.pdf
100100-07-1/mnt/p06/Users/Sarah M/Downloads/Bibliography - Snowy Owl 14 April 2
014 - GLOW posting.xls
100100-07-1/mnt/p06/Users/Sarah M/Downloads/Owl_Emergency_Care.pdf
100100-07-1/mnt/p06/Users/Sarah M/Downloads/Owl_Keeping.pdf
```

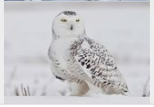
Filesystem Timeline

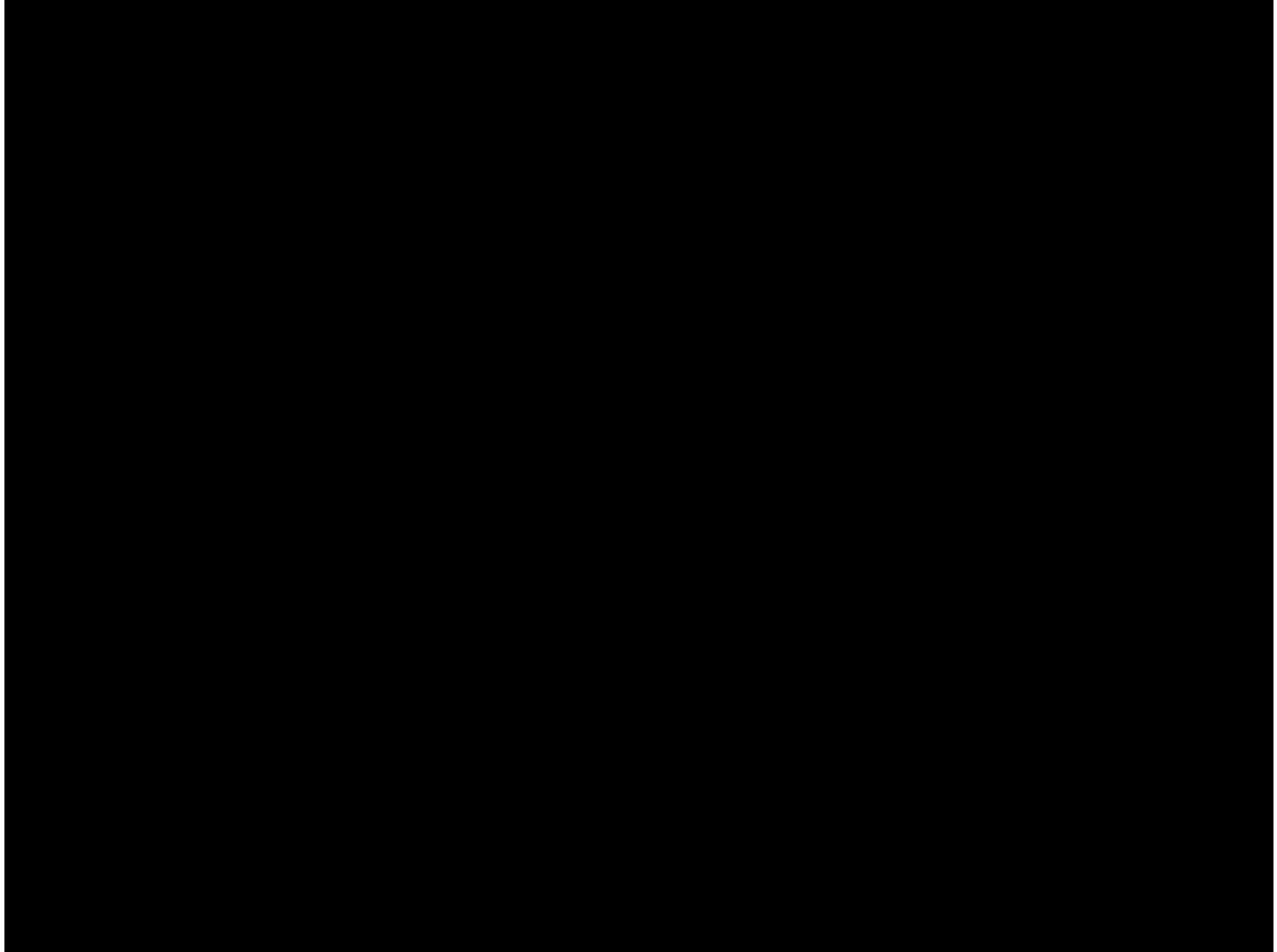
```
$ rvt2 --source 100100-07-1 -j fs_timeline
$ rvt2 --source 100100-07-1 -j events.timeline
```



RVT Analyzer. *Owl* key search

```
$ rvt2 --source 100100-07-1 -j indexer.save_directory
```

combo(28)	9.118456	***content***: (),this.editMenu.close(),this.appContext.getView("*feather*-aviary-view f.fire("subviewViewEvent","make in view",n),e.use("*feather*-aviary-view	Tags
combo(28)	9.118456	***content***: (),this.editMenu.close(),this.appContext.getView("*feather*-aviary-view f.fire("subviewViewEvent","make in view",n),e.use("*feather*-aviary-view	Tags
/embedded-1 (inside *Bibliography - Snowy Owl 14 April 2014 - GLOW posting.xls*)	9.331031	***path***: /p06/Users/Sarah M/Downloads/Bibliography - Snowy *Owl* ***filename***: Bibliography - Snowy *Owl* 14 April 2014 - GLOW posting.xls	Tags
Great Horned Owl Info.lnk	9.331031	***path***: AppData/Roaming/Microsoft/Windows/Recent/Great Horned *Owl* ***filename***: Great Horned *Owl* Info.lnk	Tags
Snowy Owl Care.lnk	10.073285	***path***: M/AppData/Roaming/Microsoft/Windows/Recent/Snowy *Owl* ***filename***: Snowy *Owl* Care.lnk	Tags
Snowy Owl 3.jpg	10.154173		Tags
Snowy Owl 4.jpg	10.154173		Tags
Snowy Owl 2.jpg	10.154173		Seen
/Emails.xml (inside *Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags
/Emails.xml (inside *87acc1f3ad80d20125000000181f581f.Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags
/Emails.xml (inside *Unistore.zip*)	12.029369	***content***: Outlook -3336 Little *bird* "Darrin DeYoung" Outlook -2930 Re: Little *bird* "Angeline Berg adventure-works.com> You still selling that resin *bird*	Tags
what is this.html	12.118093	***content***: Tags Beta animal *bird*	Tags



AI Image Classification

```
$ rvt2 --source 100100-07-2
-j ai.classify
```

$REE3NR9.jpg

$RNOB8HB.jpg

$RWY737Y.jpg

Snowy Owl 3.jpg

Snowy Owl.jpg

My New Pet.jpg

f_000ddd

f_001b3d

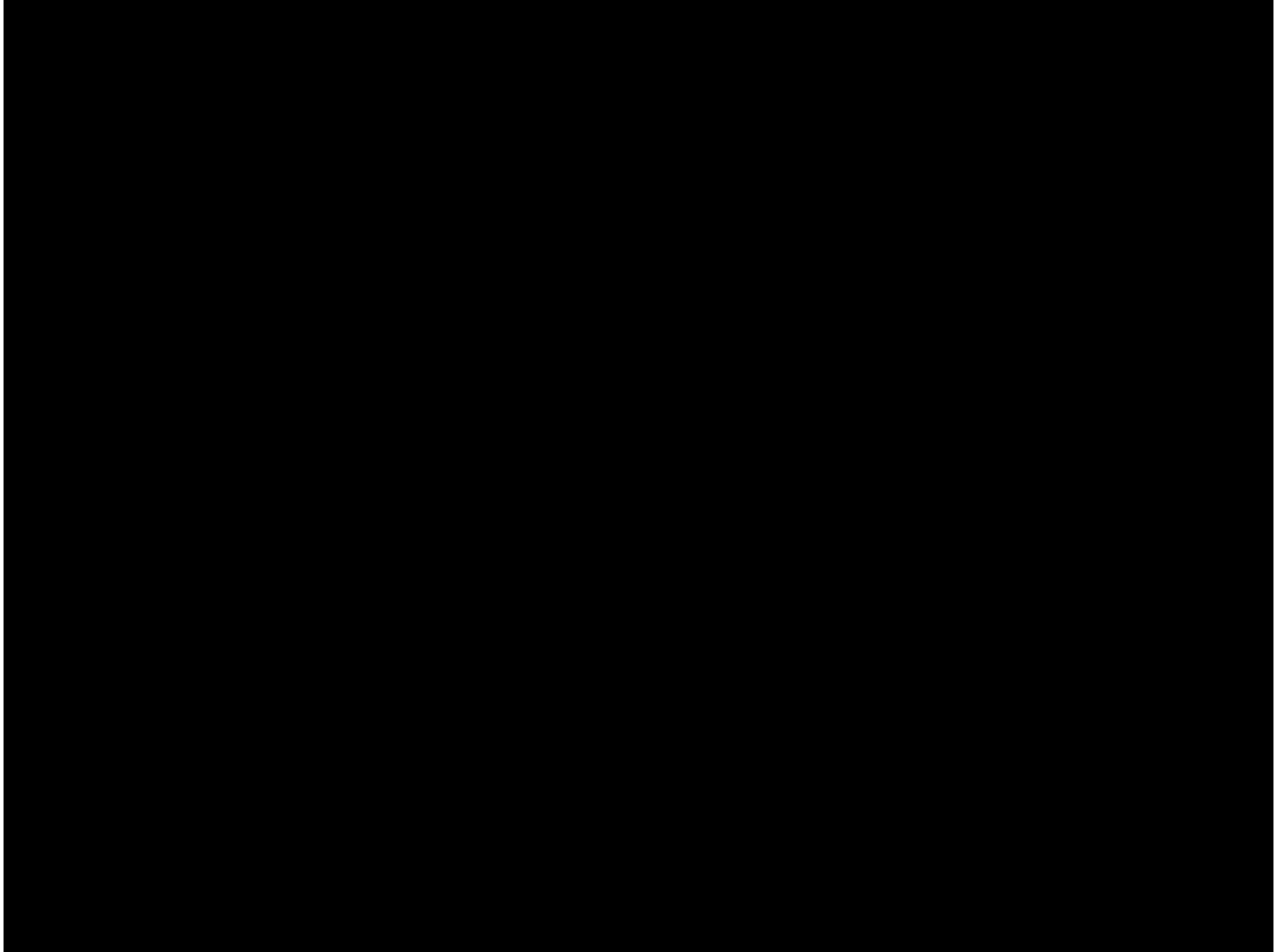
f_001b40

f_001b42

f_001b44

f_001b5f

f_001b7b



Files MFT - Kibana | Discover - Kibana | Events General - Kiban | Browsers - Kibana

kibana.incide:5601/app/kibana#/dashboard/4c85ab30-596c-11ea-bb12-0fb78935a61b?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2017-01-22T05:02:00.181

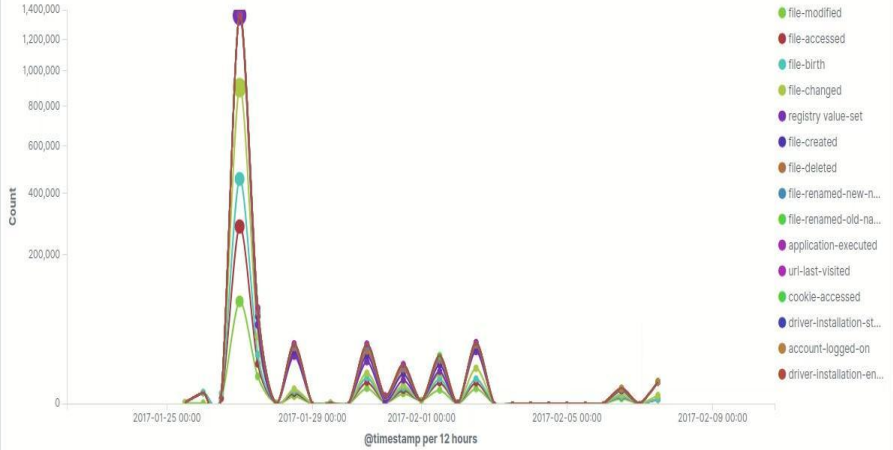
Dashboard / Events General

Full screen Share Clone Edit

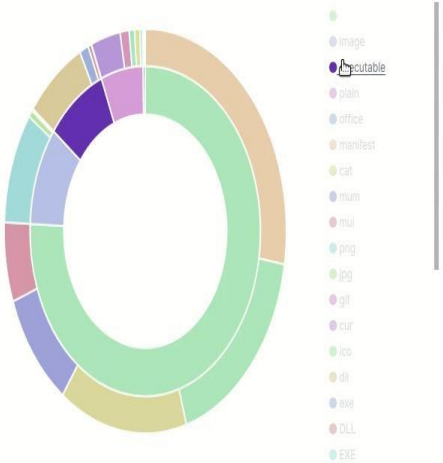
Filters Search KQL Jan 22, 2017 @ 06:02:00.1 → Feb 10, 2017 @ 16:56:52.8 Refresh

+ Add filter

Timeline by Action



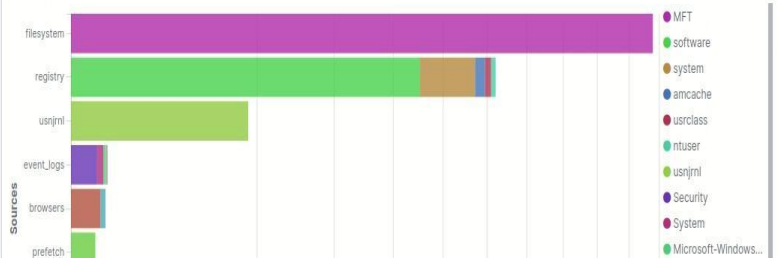
File Type



Actions

event.module.keyword: Descending	event.action.keyword: Descending	Count
filesystem	file-changed	477,768
filesystem	file-accessed	204,855
filesystem	file-birth	186,774
filesystem	file-modified	108,405
registry	registry value-set	520,917
usnjrnl	file-created	34,995
usnjrnl	file-deleted	25,669

Artifacts



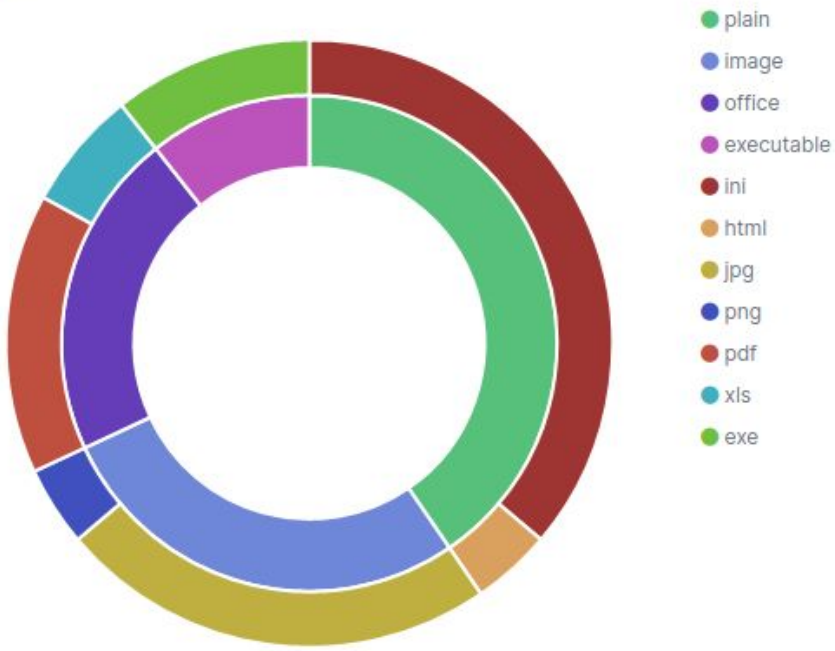
User Folder files distribution

Files Count

Directories	Count
100100-07-1/mnt/p06/Users/Sarah M/Downloads	48
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care	24
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets	16
100100-07-1/mnt/p06/Users/Sarah M/Desktop	12
100100-07-1/mnt/p06/Users/Sarah M/Desktop/WOLf Awsome_files	12
100100-07-1/mnt/p06/Users/Sarah M/Desktop/what is this_files	12
100100-07-1/mnt/p06/Users/Sarah M/Documents	8
100100-07-1/mnt/p06/Users/Sarah M	4
100100-07-1/mnt/p06/Users/Sarah M/Contacts	4
100100-07-1/mnt/p06/Users/Sarah M/Favorites	4

Export: Raw Formatted

File Type



Events associated to '*Snowy Owl Care.pdf*'

```
$ rvt2 --source 100100-07-1 -j events.save
```

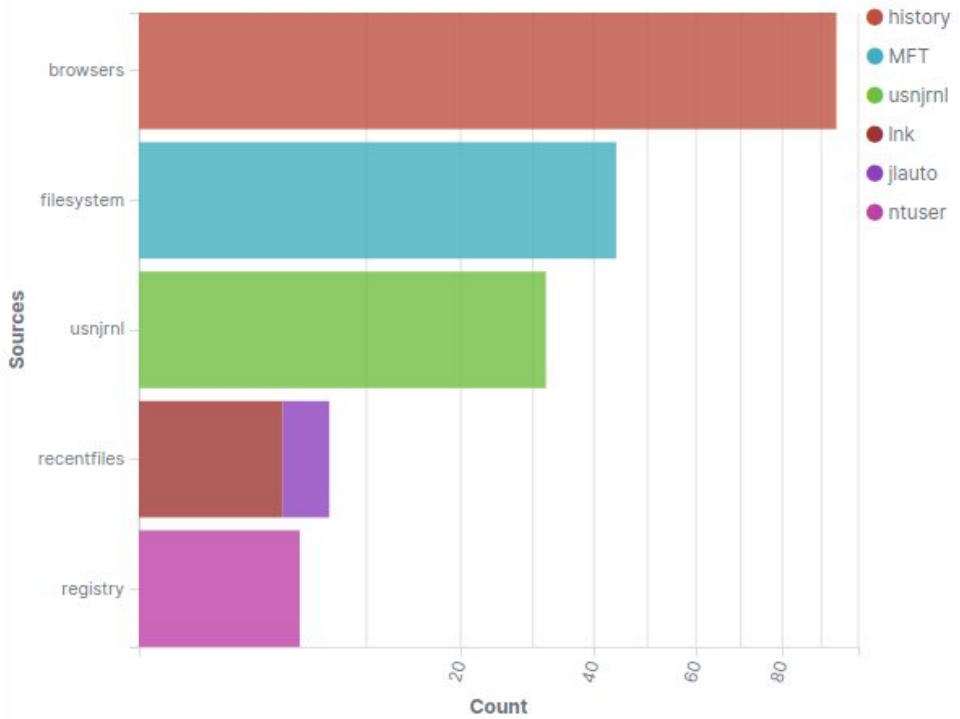
Time	event.module	message	event.dataset
Feb 2, 2017 @ 23:38:36.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.529	usnjrnl	File created: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	usnjrnl
Feb 2, 2017 @ 23:38:35.519	registry	Registry value Path set at subkey {C7DADCF6-9E6B-4B8F-8C71-E4C69FE387FE}	ntuser
Feb 2, 2017 @ 23:38:35.519	registry	Registry value DisplayName set at subkey {C7DADCF6-9E6B-4B8F-8C71-E4C69FE387FE}	ntuser
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	lnk
Feb 2, 2017 @ 23:38:35.000	recentfiles	File first opened: F:/Snowy Owl Care.pdf	lnk
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	jlauto
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	jlauto
Feb 2, 2017 @ 23:38:35.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.000	filesystem	File birth: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File modified: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File change record: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File access: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:00:17.426	usnjrnl	File created: 100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy Owl Care.pdf	usnjrnl
Feb 2, 2017 @ 23:00:17.000	filesystem	File birth: 100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy Owl Care.pdf	MFT

Events Count by Artifact and action (filtered by *Owl*)

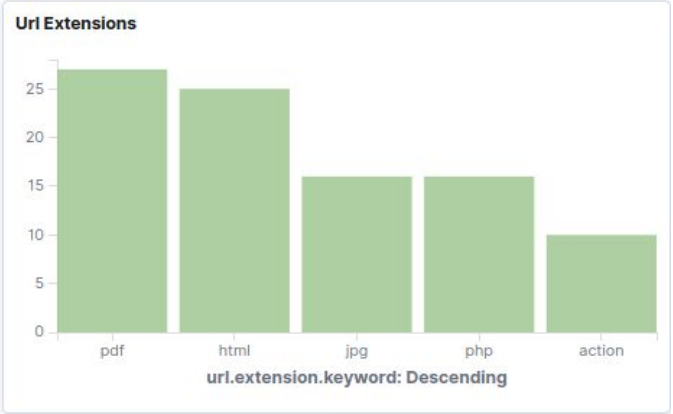
Actions

event.module.keyword: Descending	event.action.keyword: Descending	Count
browsers	url-last-visited	94
filesystem	file-accessed	11
filesystem	file-birth	11
filesystem	file-changed	11
filesystem	file-modified	11
usnjrnl	file-renamed-new-name	22
usnjrnl	file-renamed-old-name	8
usnjrnl	file-created	2
recentfiles	file-last-opened	5
recentfiles	file-first-opened	2
registry	registry value-set	5

Artifacts



Browsers History by url



Browsers Downloads

```
rvt2 --source 100100-07-1 -j browsers
```

```
$ cut -d ';' -f1,2,3,4 100100-07-1/output/browsers/downloads.csv | grep -i owl
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Great Horned Owl
.jpg";64476;"2017-01-27 17:19:12"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Pygmy Owl.jpg";9
4519;"2017-01-27 17:19:16"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Snowy Owl.jpg";5
948982;"2017-01-27 17:19:18"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Snowy Owl 2.jpg"
;10051;"2017-01-27 17:33:22"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Snowy Owl 3.jpg"
;74943;"2017-01-27 17:33:24"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads\Snowy Owl 4.jpg"
;3496271;"2017-01-27 17:33:24"
```

Recent opened files

```
$ rvt2 --source 100100-07-1 -j windows.recentfiles
```

Jan 31, 2017 @ 20:15:03.000	C:/Users/Sarah M/Documents/New Pet Care/Snowy_Owl.pdf	0x14412537	Quick Access
Jan 31, 2017 @ 20:12:19.000	F:/Snowy_Owl.pdf	0x80bc89a2	
Jan 31, 2017 @ 20:10:30.000	C:/Users/Sarah M/Documents/New Pet Care/Owl_Emergency_Care.pdf	0x14412537	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116
Jan 31, 2017 @ 20:09:10.000	C:/Users/Sarah M/Downloads/Owl_Keeping.pdf	0x14412537	
Jan 31, 2017 @ 20:09:10.000	C:/Users/Sarah M/Downloads/Owl_Keeping.pdf	0x14412537	
Jan 31, 2017 @ 20:09:10.000	C:/Users/Sarah M/Downloads/Owl_Keeping.pdf	0x14412537	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116
Jan 31, 2017 @ 20:09:10.000	C:/Users/Sarah M/Downloads/Owl_Keeping.pdf	0x14412537	Quick Access
Jan 31, 2017 @ 20:08:59.000	C:/Users/Sarah M/Documents/New Pet Care/Owl_Emergency_Care.pdf	0x14412537	
Jan 31, 2017 @ 20:08:59.000	C:/Users/Sarah M/Downloads/Owl_Emergency_Care.pdf	0x14412537	Google Chrome 9.0.597.84 / 12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116
Jan 31, 2017 @ 20:08:59.000	C:/Users/Sarah M/Downloads/Owl_Emergency_Care.pdf	0x14412537	Quick Access
Jan 27, 2017 @ 18:23:32.000	C:/Users/Sarah M/Desktop/pets/Great Horned Owl.jpg	0x14412537	
Jan 27, 2017 @ 18:23:29.000	C:/Users/Sarah M/Desktop/pets/Pygmy Owl.jpg	0x14412537	Photos Microsoft 16.526.11220.0 (Windows 10)
Jan 27, 2017 @ 18:23:29.000	C:/Users/Sarah M/Desktop/pets/Pygmy Owl.jpg	0x14412537	
Jan 27, 2017 @ 18:23:29.000	C:/Users/Sarah M/Desktop/pets/Pygmy Owl.jpg	0x14412537	
Jan 27, 2017 @ 18:23:25.000	C:/Users/Sarah M/Desktop/pets/Snowy Owl.jpg	0x14412537	Photos Microsoft 16.526.11220.0 (Windows 10)
Jan 27, 2017 @ 18:23:25.000	C:/Users/Sarah M/Desktop/pets/Snowy Owl.jpg	0x14412537	
Jan 27, 2017 @ 18:23:25.000	C:/Users/Sarah M/Desktop/pets/Snowy Owl.jpg	0x14412537	
Jan 27, 2017 @ 18:23:25.000	C:/Users/Sarah M/Desktop/pets/Snowy Owl.jpg	0x14412537	Quick Access
Jan 27, 2017 @ 18:23:03.000	C:/Users/Sarah M/Desktop/pets/Great Horned Owl.jpg	0x14412537	Photos Microsoft 16.526.11220.0 (Windows 10)

Strings Search

```
$ rvt2 --source 100100-07-2 -j strings
$ rvt2 --source 100100-07-2 -j search_strings
```

```
Pt: p06; Blk:
59464710; Inode:  Not Allocated; File:

..'.#.../š[.,.............(....
.A.......q.................a......N..........99..Y.... .....m.'x..Ž......
.........q.........š.....*..|Dw..d..|Dw..d..|Dw..*..|Dw..........._......
.  .....................U.s.e.r.s./.S.a.r.a.h. .M.c.A.v.o.y./.A.p.p.D.a
.t.a./.L.o.c.a.l./.P.a.c.k.a.g.e.s./.M.i.c.r.o.s.o.f.t...M.i.c.r.o.s.o.f
.t.E.d.g.e._.8.w.e.k.y.b.3.d.8.b.b.w.e./.A.C./.#.!.0.0.1./.M.i.c.r.o.s.o
.f.t.E.d.g.e./.C.a.c.h.e./.1.7.R.B.X.P.H.R./.n.a.v.i.g.a.t.i.o.n.[.1.)..
.j.s......š[.,.....'.#...)š[.,.............(.....A.......p.......M+.....
..a......N..........99..Y.... .....m.'x..................p.............
.........u..................&Gw....v'Gw....v'Gw.....&Gw.................
.  .........................D...U.s.e.r.s./.S.a.r.a.h. .M.c.A.v.o.y./.A
.p.p.D.a.t.a./.L.o.c.a.l./.P.a.c.k.a.g.e.s./.M.i.c.r.o.s.o.f.t...M.i.c.r
.o.s.o.f.t.E.d.g.e._.8.w.e.k.y.b.3.d.8.b.b.w.e./.A.C./.#.!.0.0.1./.M.i.c
.r.o.s.o.f.t.E.d.g.e./.C.a.c.h.e./.1.7.R.B.X.P.H.R.N.o.c.t.u.r.n.a.l.[.1
.)...h.t.m.N.O.C.T.U.R...1...H.T.M.......š[.,.....'.#....š[.,..........
...(.....A.......p.......M+.......b......N..........99..Y.... .....m.'x.
```

/Rooted

Android Device Analysis

$ rvt2 --source 100100-07-2 -j android.databases

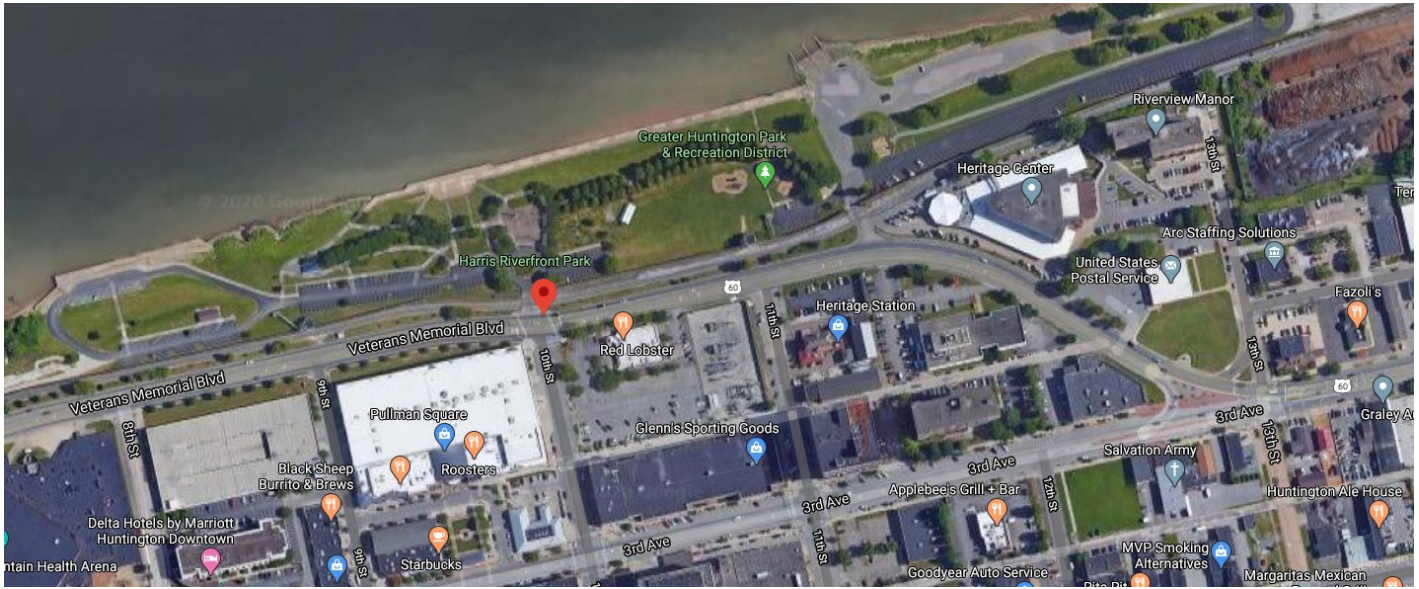
```
$ cut -d';' -f1,2,3,4 100100-07-2/output/android/applications_state.csv | head -10
"package_name";"title";"version";"first_downloaded"
"com.cmcm.locker";"CM Locker-AppLock,ScreenLock";45043237;"2017-01-30 22:16:09"
"com.cleanmaster.security";"CM Security AppLock AntiVirus";30245023;"2017-01-30 22:14:26"
"com.zhiliaoapp.musically";"musical.ly";2017020301;"2017-01-30 21:59:54"
"com.google.android.play.games";"Google Play Games";39080038;"2017-01-25 20:50:21"
"com.skype.raider";"Skype - free IM & video calls";119604041;"2017-01-25 02:18:55"
"com.enflick.android.TextNow";"TextNow - free text + calls";11192;"2017-01-24 15:51:40"
"com.twitter.android";"Twitter";6110047;"2017-01-24 15:51:01"
"com.snapchat.android";"Snapchat";1025;"2017-01-24 15:49:52"
"com.facebook.katana";"Facebook";48723175;"2017-01-24 15:47:53"
```

Evidences:

```
$ grep -i delivery 100100-07-2/output/android/sms.csv
"2017-02-01 00:41:15";"+13045184333";"";1;1;"Sarah, the delivery is
 today 7 tonight the confirmation will come later through pidgin";"
+12404492167"
```

```
$ grep Layster82 100100-07-2/output/android/contacts_plus.csv
"1f3503d78d1f621b";"Layla Aster";"Layster82@gmail.com";"2017-01-27
17:26:54"
```

Maps and Navigation




```
$ srch_strings 100100-07-2/mnt/p31/data/com.google.android.apps.maps/databases
/gmm_storage.db-journal
http://maps.google.com/?q=Harris+Riverfront+Park+loc:+Veterans+Memorial+Blvd
,+Huntington,+WV+25701&gl=US&sll=38.423656,-82.442845:
```

/Rooted®

Conclusions

- Numerous documents related to owls have been identified in the analyzed devices.
- Traces of Internet searches related to owl purchasing have been found on both the analyzed computer and the mobile phone.
- Traces of emails with owl purchasing topic have been found on the computer
- On **January 30**, 2017, the purchase of an owl is agreed by ***Sarah McAvoy***, the main user of the application musically on the Android device analyzed and matching on behalf of the user of the Windows PC. The animal belongs to the user ***layster82***, named Layla and email *Layster82gmail*.
- The purchase price is agreed at a value of **5000** and a face-to-face meeting is set at the ***Harris river front park*** location.
- The meeting point mentioned in the sales conversation, located in Huntington, was searched in the Google Maps application, as well as instructions on how to get there.
- An SMS message is identified from the telephone number **+13045184333** in which the time of delivery is set at 7 PM.
- The email ***Layster82@gmail.com*** is identified among the contacts of the investigated device, and can be associated with the name ***Layla Aster***.
- Just after these events, Sarah McAvoy googles how to feed an owl.

Installation

Installation and repos

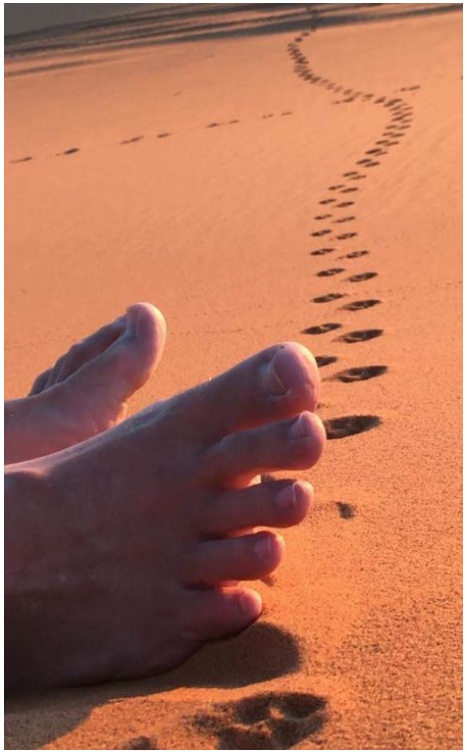
```
git clone https://github.com/IncideDigital/rvt2-docker.git
cd rvt2-docker
./rvt2
```

Documentation: https://github.com/IncideDigital/rvt2-docs

Source code: https://github.com/IncideDigital/rvt2

Docker: https://github.com/IncideDigital/rvt2-docker

Next steps



New modules!

New artifacts!

New GUIs!

Better Incident Response!

Better documentation!

Your collaboration!

Thanks!

Run a DFIR investigation the easy way: Revealer Toolkit 2

Abraham Pasamar
Juan Vera