INTRODUCTION À LA FORENSIC

SOUTENANCE DE STAGE

Cherrier Martin
10 semaines

Tuteur : Eddy Godelle
Maitre de stage : Christophe Rosenberger

SOMMAIRE

PRÉSENTATION DU LABORATOIRE

Laboratoire de recherche

PLUSIEURS TUTELLES, DIFFÉRENTS SITES

Divisé en équipes

SAFE, CODAG, AMACC, MAD, IMAGE ...

Différents sujets et projets

FORENSIC, BIOMÉTRIE, G'DIP, GMIC

PRÉSENTATION SAFE

- Équipe de chercheurs
- Différents sujets étudiés
- Des projets variés

FORENSIQUE ?

SCIENCE DE RECOUVREMENT DE DONNÉES

Analyse(s) de supports

RÉCUPÉRATION, ISOLEMENT, AUTHENTICITÉ

5 Étapes nécessaires

IDENTIFICATION, PRÉSERVATION ...

Objectifs judiciaires

MAIS AUSSI DE SAUVEGARDE ET DE PROTECTION

PRÉSENTATION G'DIP

Interface Web Modulable

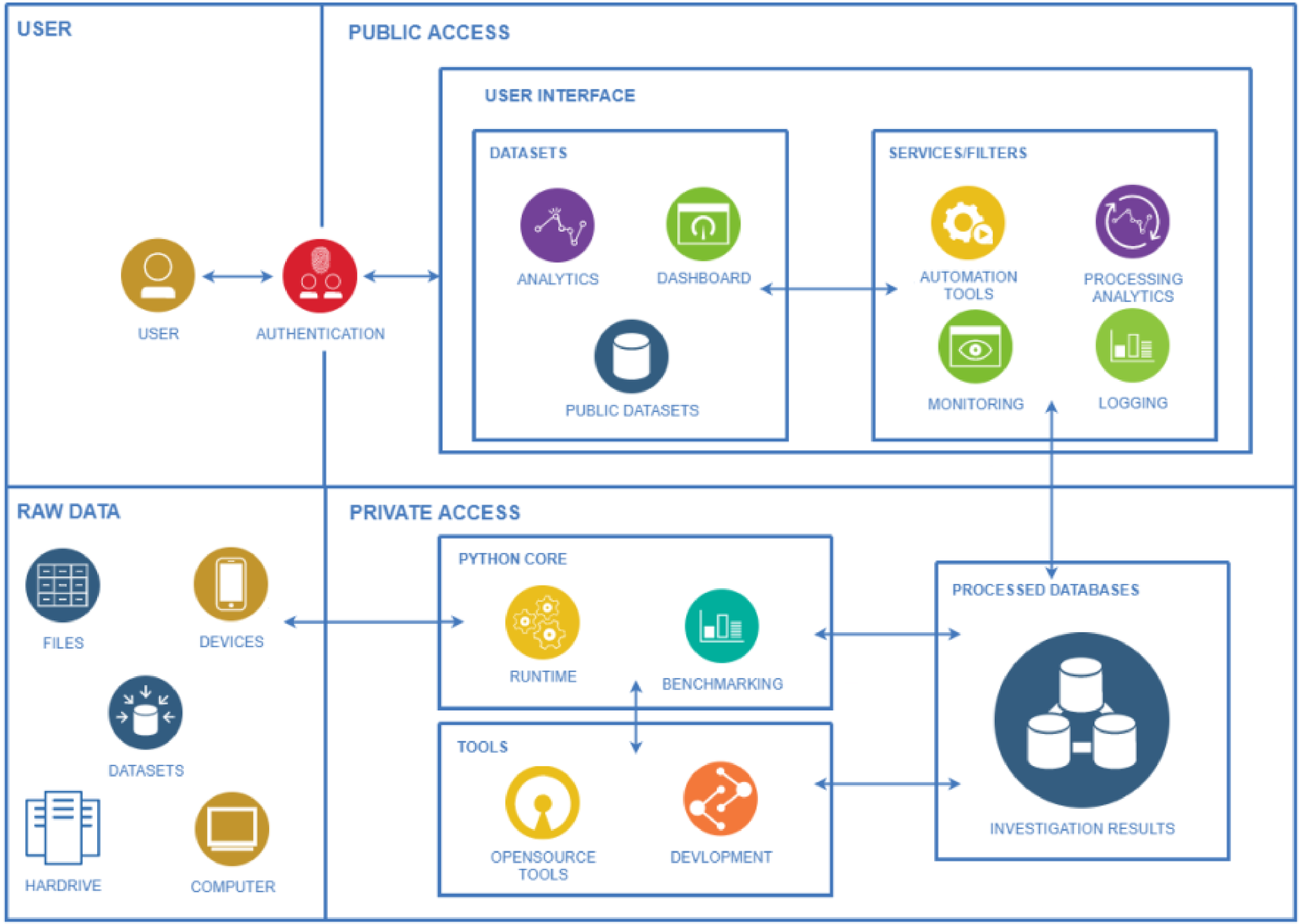
DIFFÉRENTS FILTRES, GRAPHIQUES

Introduction à la forensic

INTERFACE POUR DÉBUTANTS

Différentes utilisations

PROFESSIONNELS, PARTICULIERS,


USER
PUBLIC ACCESS
USER INTERFACE
DATASETS
ANALYTICS
DASHBOARD
PUBLIC DATASETS
SERVICES/FILTERS
AUTOMATION TOOLS
PROCESSING ANALYTICS
MONITORING
LOGGING
USER
AUTHENTICATION
RAW DATA
FILES
DEVICES
DATASETS
HARDRIVE
COMPUTER
PRIVATE ACCESS
PYTHON CORE
RUNTIME
BENCHMARKING
TOOLS
OPENSOURCE TOOLS
DEVLOPMENT
PROCESSED DATABASES
INVESTIGATION RESULTS

Gdip About us Contact us Login

Summary Analysis Index

171 / 5500

1 Filtre actif x

File 1 x

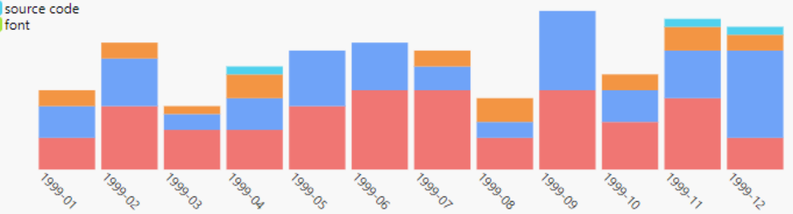
Image

text
image
application
autre

Classes

Années> Mois

text
image
application
video
audio
source code
font



Historique :

0 Created at

demo **Name**
4.16 **Go**
23 **Folders**
5500 **Files**
16 **Filtres disponibles**

100

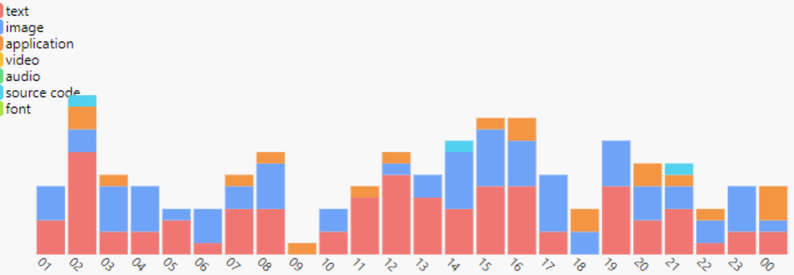
First Date 1990-01-05
Last Date 2023-04-24
Class 6
Extension 45
Mimetype 33

Folders

- **demo** dossier: 22 fichier: 0
  - + **2000** dossier: 10 fichier: 0
  - - **1990** dossier: 2 fichier: 0
    - + **1996-1999** dossier: 0 fichier: 15
    - + **1991-1995** dossier: 0 fichier: 1
  - + **documents** dossier: 1 fichier: 35
  - + **total** dossier: 0 fichier: 16
  - + **images** dossier: 3 fichier: 13
  - + **compt** dossier: 0 fichier: 25

Heure

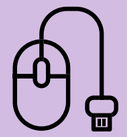
text
image
application
video
audio
source code
font



OBJECTIFS

Documentation & Méthodologie

1



Tests de l'interface

2

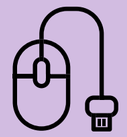
Compréhension FRED

3

MES MISSIONS

Rédactions de documents

1



Tests & Retours

2

Analyse de supports de données

3

Machine FRED

Forensic Recovery Evidence Device

Baie 4D

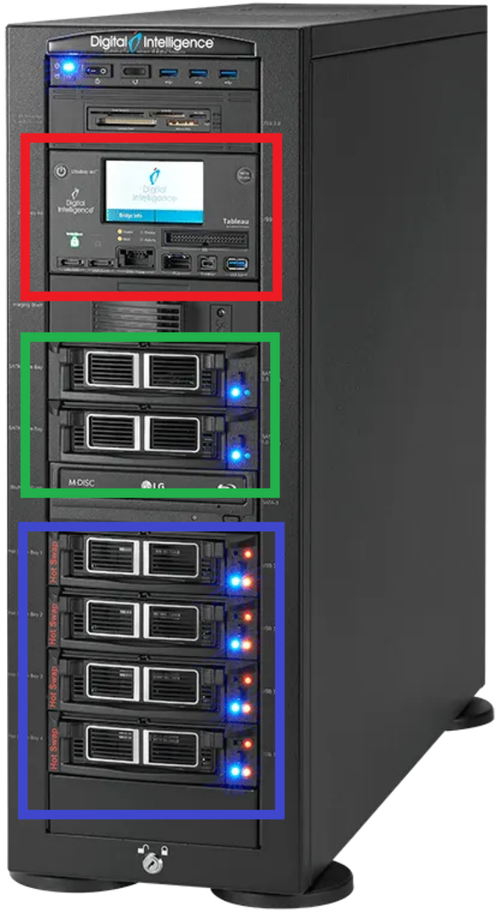
PORTS BLOQUEURS D'ÉCRITURE
ÉCRAN AFFICHANT DES INFORMATIONS

Stockage fixe

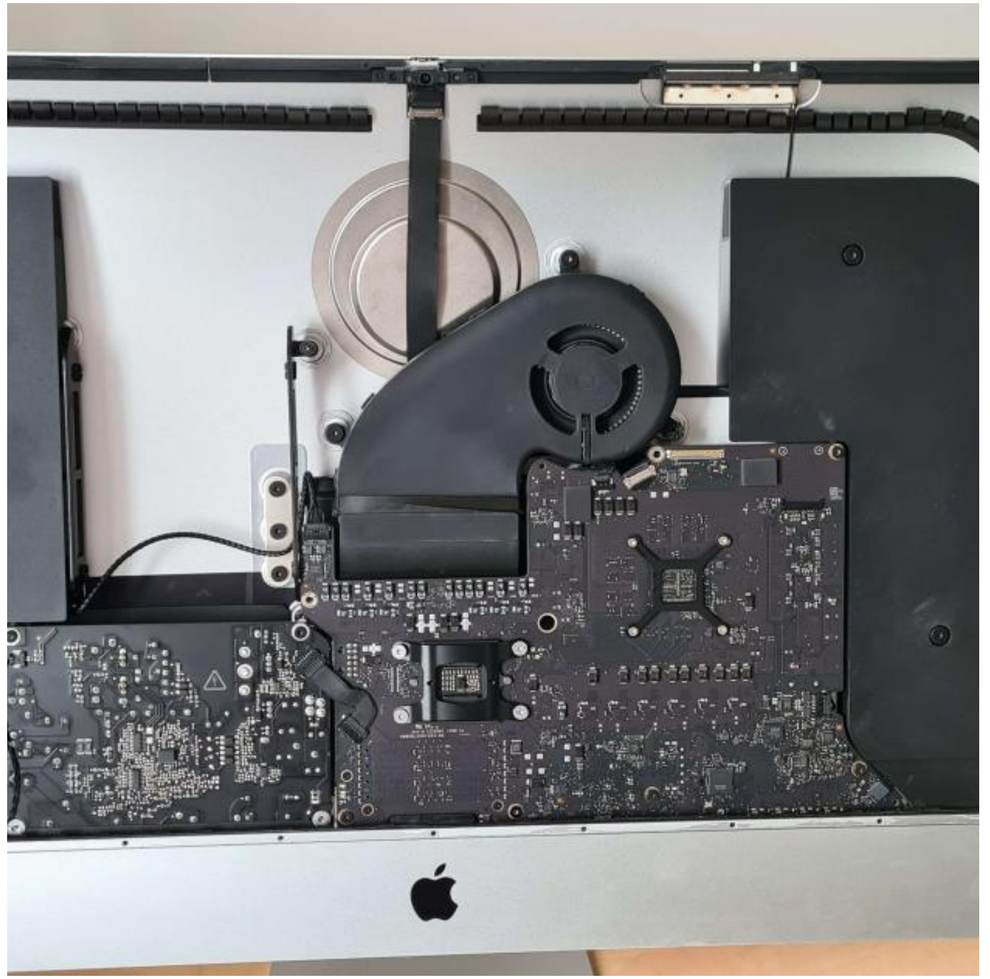
RACKS VIDES - AJOUT DE SUPPORTS

Partie amovible

AJOUTS D'OUTILS ET D'INTERFACES




160GB
Maxtor
WD Western Digital
WD Caviar Blue



Autopsy

Logiciel d'analyse

Logiciel Open-Source

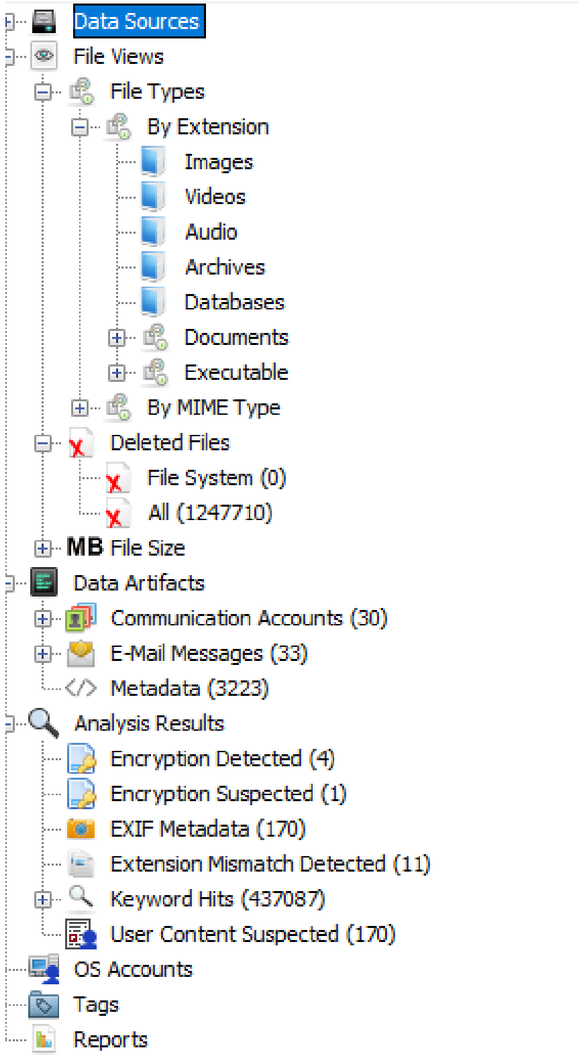
BASÉ SUR LA SUITE SLEUTH-KIT

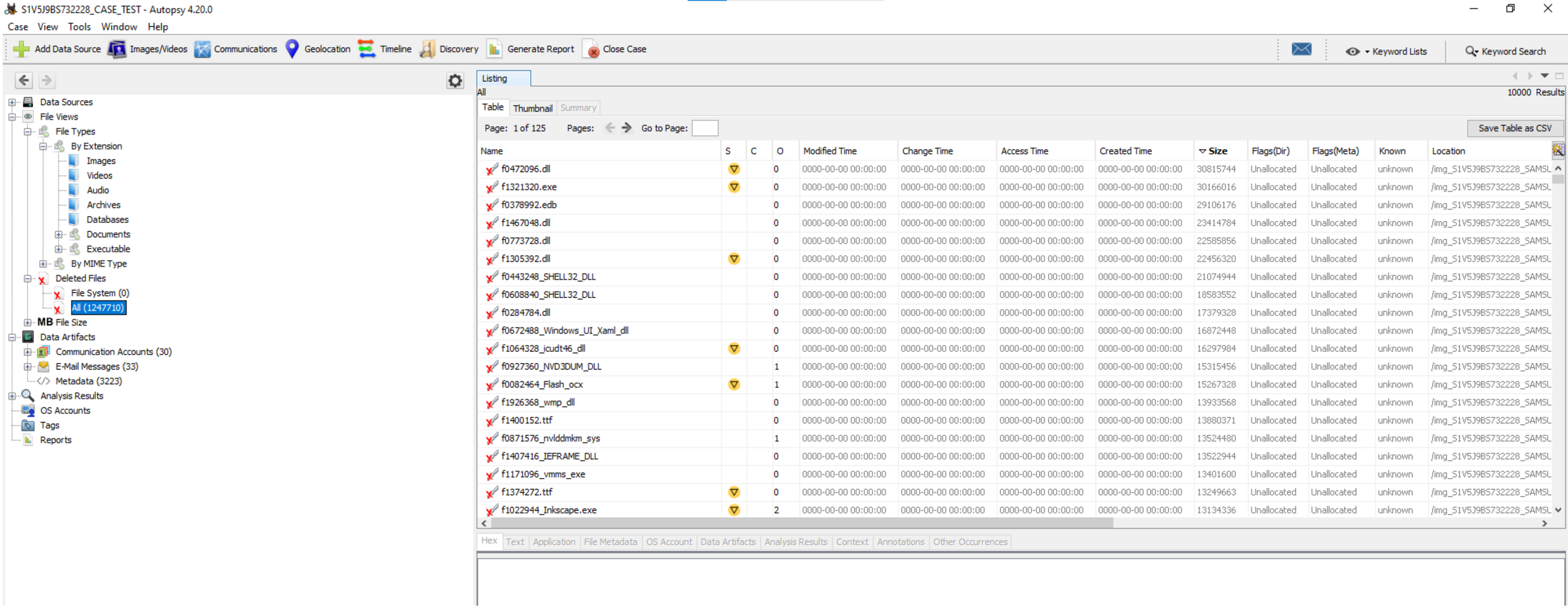
Différents outils d'analyse

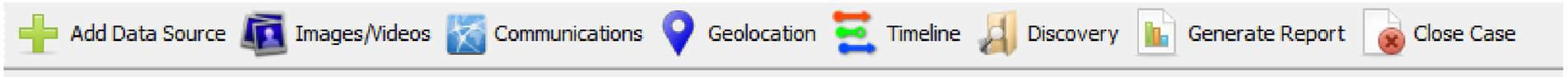
CARTE DE GÉOLOCALISATION
VISUALISATION DE MAILS

Modulable à volonté

MODULES PROGRAMMABLES
OU TÉLÉCHARGEABLES




S1V5J9BS732228_CASE_TEST - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
File Types
By Extension
Images
Videos
Audio
Archives
Databases
Documents
Executable
By MIME Type
Deleted Files
File System (0)
All (1247710)
MB File Size
Data Artifacts
Communication Accounts (30)
E-Mail Messages (33)
Metadata (3223)
Analysis Results
OS Accounts
Tags
Reports
Listing
All
10000 Results
Table Thumbnail Summary
Page: 1 of 125 Pages: Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location
f0472096.dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 30815744 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1321320.exe 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 30166016 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0378992.edb 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 29106176 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1467048.dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 23414784 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0773728.dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 22585856 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1305392.dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 22456320 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0443248_SHELL32_DLL 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 21074944 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0608840_SHELL32_DLL 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 18583552 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0284784.dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 17379328 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0672488_Windows_UI_Xaml_dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 16872448 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1064328_icudt46_dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 16297984 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0927360_NVD3DUM_DLL 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 15315456 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0082464_Flash_ocx 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 15267328 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1926368_wmp_dll 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13933568 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1400152.ttf 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13880371 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f0871576_nvlddmkm_sys 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13524480 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1407416_IEFRAME_DLL 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13522944 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1171096_vmms_exe 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13401600 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1374272.ttf 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13249663 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
f1022944_Inkscape.exe 2 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13134336 Unallocated Unallocated unknown /img_S1V5J9BS732228_SAMSL
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case

RÉSULTATS

Machine FRED

- Introduction à la forensique
- Découverte du fonctionnement

Tests & retours

- Nombreux bugs découvert
- Ajouts sur l'interface

Documentation & méthodologie

- Procédures rédigées
- Recherches et documentations disponibles

CE QUE LE STAGE M'A APPORTÉ

1

RECHERCHE

Méthodes
Documentations
Tests

2

AUTONOMIE

Travail autonome
Développement d'idées
Adaptabilité

3

SYNTHÉTISER

Vulgarisation
Sujets complexes

4

EFFICACITÉ

Travail rapide
Soigné

5

VIE D'ÉQUIPE

Réunions d'équipe
Socialisation
Entraide

CONCLUSION

Expérience

- Différentes tâches
- Monde scientifique

Échanges

- Avec des chercheurs
- Avec des membres de l'ENSI

Projet(s) futur(s)

- Monde de la recherche
- École d'ingénieur

Merci à tous

Listing

All

10000 Results

Table | Thumbnail | Summary

Page: 1 of 125 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0472096.dll	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30815744	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1321320.exe	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30166016	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0378992.edb			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29106176	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1467048.dll			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23414784	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0773728.dll			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22585856	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1305392.dll	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22456320	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0443248_SHELL32_DLL			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	21074944	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0608840_SHELL32_DLL			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18583552	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0284784.dll			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17379328	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0672488_Windows_UI_Xaml_dll			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16872448	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1064328_icudt46_dll	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16297984	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0927360_NVD3DUM_DLL			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15315456	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0082464_Flash_ocx	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15267328	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1926368_wmp_dll			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13933568	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1400152.ttf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13880371	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f0871576_nvlddmkm_sys			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13524480	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1407416_IEFRAME_DLL			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13522944	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1171096_vmms_exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13401600	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1374272.ttf	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13249663	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL
f1022944_Inkscape.exe	▽		2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13134336	Unallocated	Unallocated	unknown	/img_S1V5J9BS732228_SAMSL

Listing

Default

33 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
f1725760.mbox				; >;	webmaster@python.org;	Banned file: auto__mail.python.bat in mail from you	2004-11-27 04:41:44 CET	BANNED FILENAME ALERTYour message to: xxxx
f1725568.mbox				MAILER-DAEMON@zinfandel.lacita.com;	linuxuser-admin@www.linux.org.uk;	Returned mail: Too many hops 19 (17 max): from <linuxus...	2001-04-06 19:23:06 CEST	This is a MIME-encapsulated message--JAB03225
f0931888.mbox				MAILER-DAEMON@zinfandel.lacita.com;	linuxuser-admin@www.linux.org.uk;	Returned mail: Too many hops 19 (17 max): from <linuxus...	2001-04-06 19:23:06 CEST	This is a MIME-encapsulated message--JAB03225
f0931832.mbox				; >;	webmaster@python.org;	Banned file: auto__mail.python.bat in mail from you	2004-11-27 04:41:44 CET	BANNED FILENAME ALERTYour message to: xxxx
f1701272.mbox				; >;	webmaster@python.org;	Banned file: auto__mail.python.bat in mail from you	2004-11-27 04:41:44 CET	BANNED FILENAME ALERTYour message to: xxxx
f1701224.mbox				MAILER-DAEMON@zinfandel.lacita.com;	linuxuser-admin@www.linux.org.uk;	Returned mail: Too many hops 19 (17 max): from <linuxus...	2001-04-06 19:23:06 CEST	This is a MIME-encapsulated message--JAB03225
f1943256.mbox				adminlinux@e110pc04;	root@e110pc04;	*** SECURITY information for hplaurent ***	2010-06-25 09:51:55 CEST	hplaurent : juin 25 09:51:55 : adminlinux :
f1943256.mbox				adminlinux@e110pc04;	root@e110pc04;	*** SECURITY information for hplaurent ***	2010-06-25 09:54:51 CEST	hplaurent : juin 25 09:54:51 : adminlinux :
f1943256.mbox				root@e110pc04;	root@e110pc04;	Cron <root@e105pc11> start -q anacron || :	2011-12-07 07:30:01 CET	start: Job is already running: anacron
f1943256.mbox				root@e110pc04;	root@e110pc04;	Cron <root@e105pc11> start -q anacron || :	2011-12-16 07:30:01 CET	start: Job is already running: anacron
f1943256.mbox				root@e110pc04;	root@e110pc04;	Cron <root@e105pc11> start -q anacron || :	2012-01-09 07:30:01 CET	start: Job is already running: anacron
f1943256.mbox				root@e110pc04;	root@e110pc04;	Cron <root@e105pc11> start -q anacron || :	2012-01-13 07:30:01 CET	
f1480456.txt						So you want to use the new Gnus		Actually, since you are reading this, chances are
f1480456.txt						Starting up		If you are having problems with Gnus not finding
f1480456.txt								
f1480456.txt								There's a whole bunch of other methods for readi
f1480456.txt						Where are all the groups, then?		If this is the first time you have used a newsreade
f1480456.txt						I want to read my mail!		Yes, Virginia, you can read mail with Gnus.First yc
f1480456.txt						Foreign newsgroups		These are groups that do not come from `gnus-se

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 4 of 6 Result

E-Mail Messages

From: root@e110pc04; 2011-12-16 07:30:01 CET

To: root@e110pc04;

CC:

Subject: Cron <root@e105pc11> start -q anacron || :

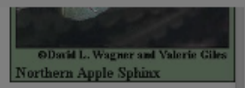
Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

start: Job is already running: anacron

py06ppbv9
586

abhg3y94i
736



x42mtfcil6
461

jvsjtr
750

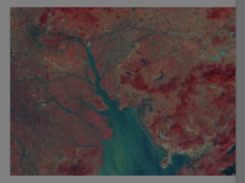
54xf0c9dd
557

u4oxjt
761

170f6cl
2959

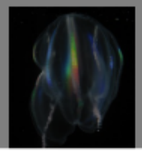
chhuplph
566

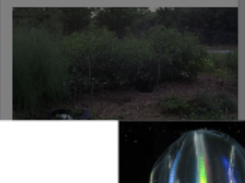
rn0r78
676



g3rstdt9z
572

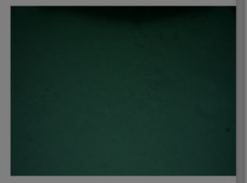
u3n
8





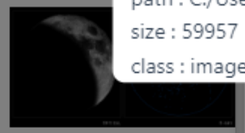
mmd2
607

lt8db4
711



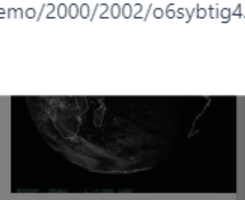
ubircq3vit
763

hnbhd7g
620

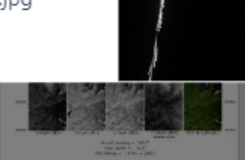


dagjnnyc
878

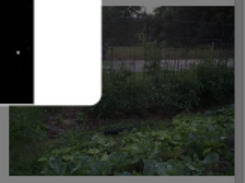
bbxhgm
833



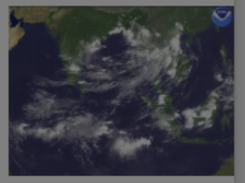
7198nm09ao
2997



2sc3hf97
2970



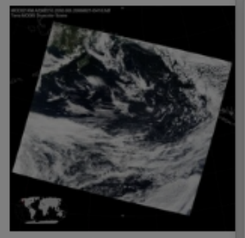
z16ehr5i8
767



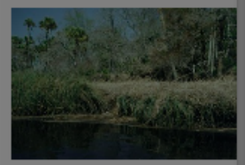
42eez2f22p
2985

79bee
3002

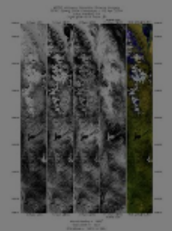
0bdkec
2954



dqspxm
786

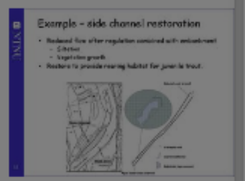


ben19
3032

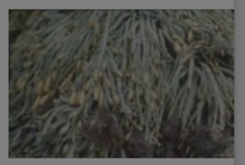


ecqncvxu
3056

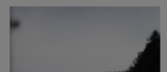
59t1wn5
2990

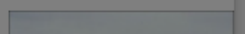


3cs792dsy
822



rwo2ud8z4
3140



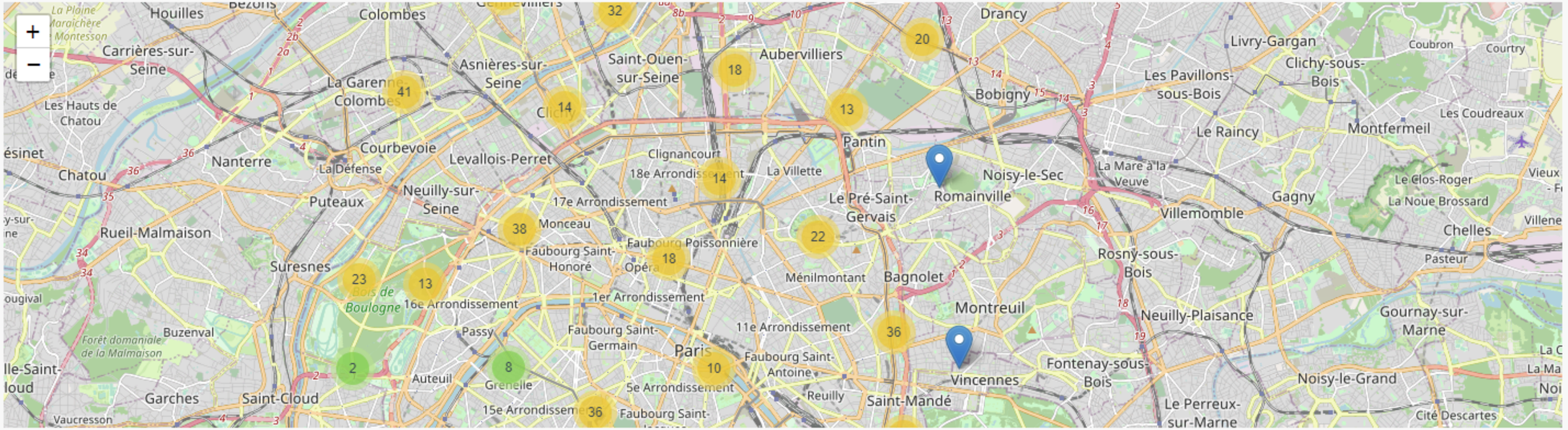


id : 625
created_at_date : 1993-04-09 11:42
created_at_time : 1970-01-01 16:51
extension : jpg
mimetype : image/jpeg
name : o6sybtig4
path : C:/Users/cardoso231/Desktop/demo/2000/2002/o6sybtig4.jpg
size : 59957
class : image

Historique :

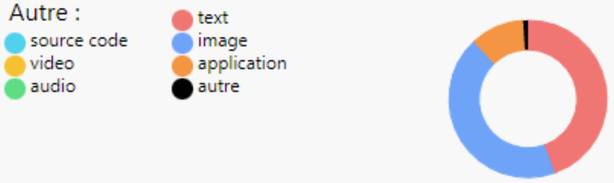
0 Created at
1 Outdoor
2 Indoor
3 Outdoor

500

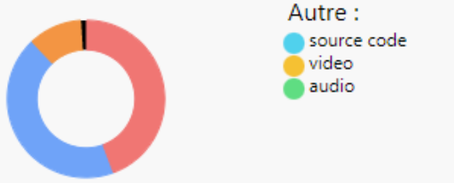


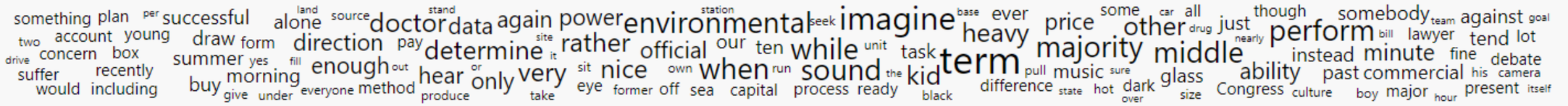
Class

Extension

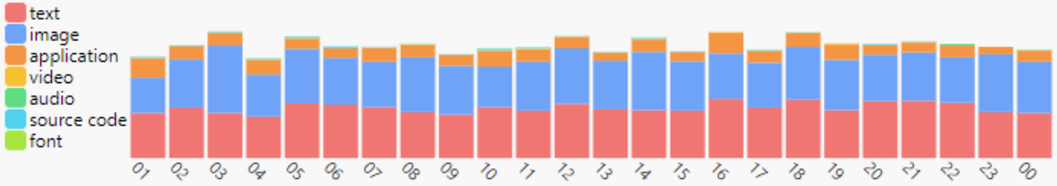


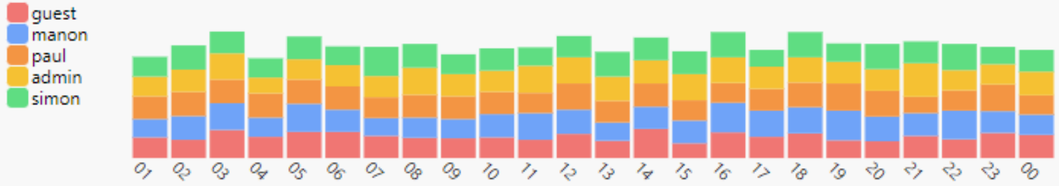
Mimetype





Heure





Heure