DIGITAL FORENSICS

Emmanuel Giguet
Christophe Rosenberger

GREYC Laboratory (UMR 6072)
UNICAEN – ENSICAEN – CNRS

Emmanuel.giguet@unicaen.fr
Christophe.rosenberger@ensicaen.fr

GREYC

GREYC

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

WHO ARE WE ?

Emmanuel Giguet

Researcher (CNRS)

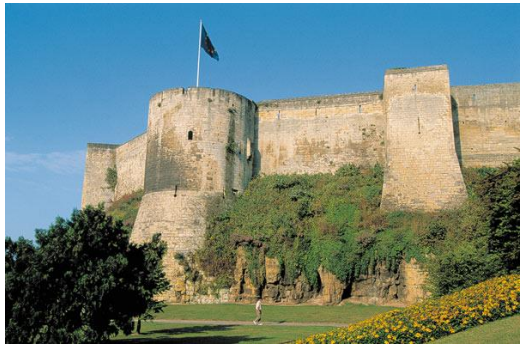
Research in natural language processing

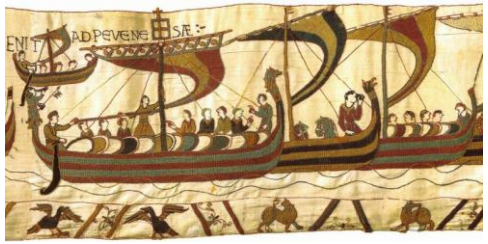
Christophe Rosenberger

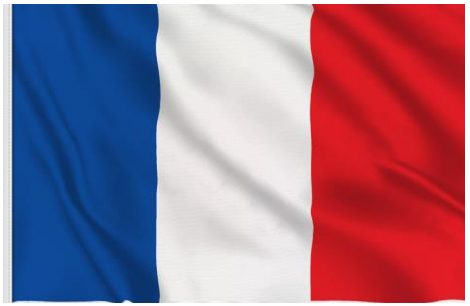
Full professor (ENSICAEN)

Research in biometrics

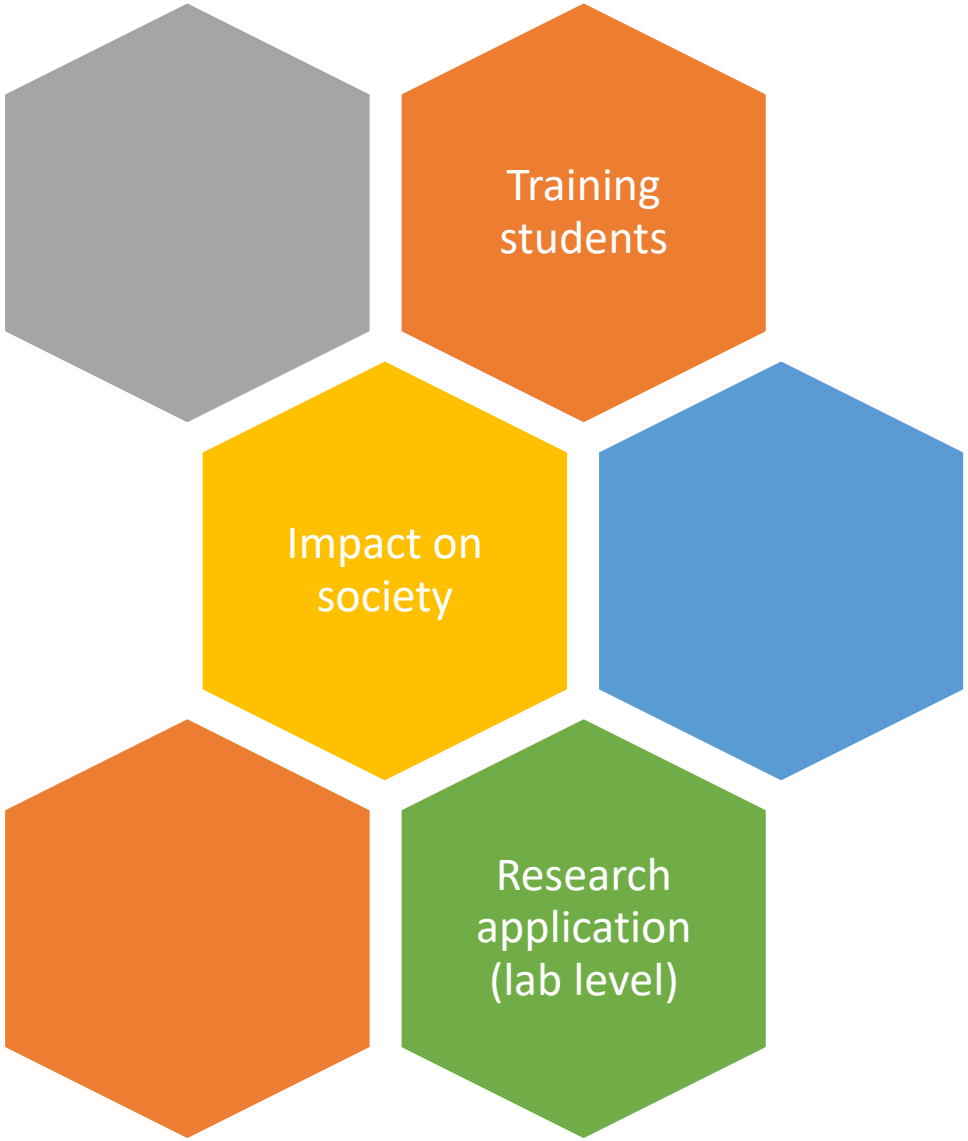
WHERE ARE WE COMING FROM?







WHY DIGITAL FORENSICS?



PLAN

- GREYC research lab
- Introduction to digital forensics
- Expert in digital forensics
- G'DIP platform
- Tools illustrations
- Perspectives

Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

GREYC RESEARCH LAB

Research in Digital Sciences

Image processing, artificial intelligence, data science, instrumentation, theoretical computer science, cybersecurity, natural language processing, digital forensics …

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

STAFF

170 Members

- 6 full time CNRS researchers
- 23 full professors
- 53 associate professors (22 HDR)
- 48 PhD students
- 19 permanent administrative and technical
- 16 post-doc and research engineers
- 12 associate members

Annual budget: 2000 K€ (without permanent salary)

https://www.greyc.fr/

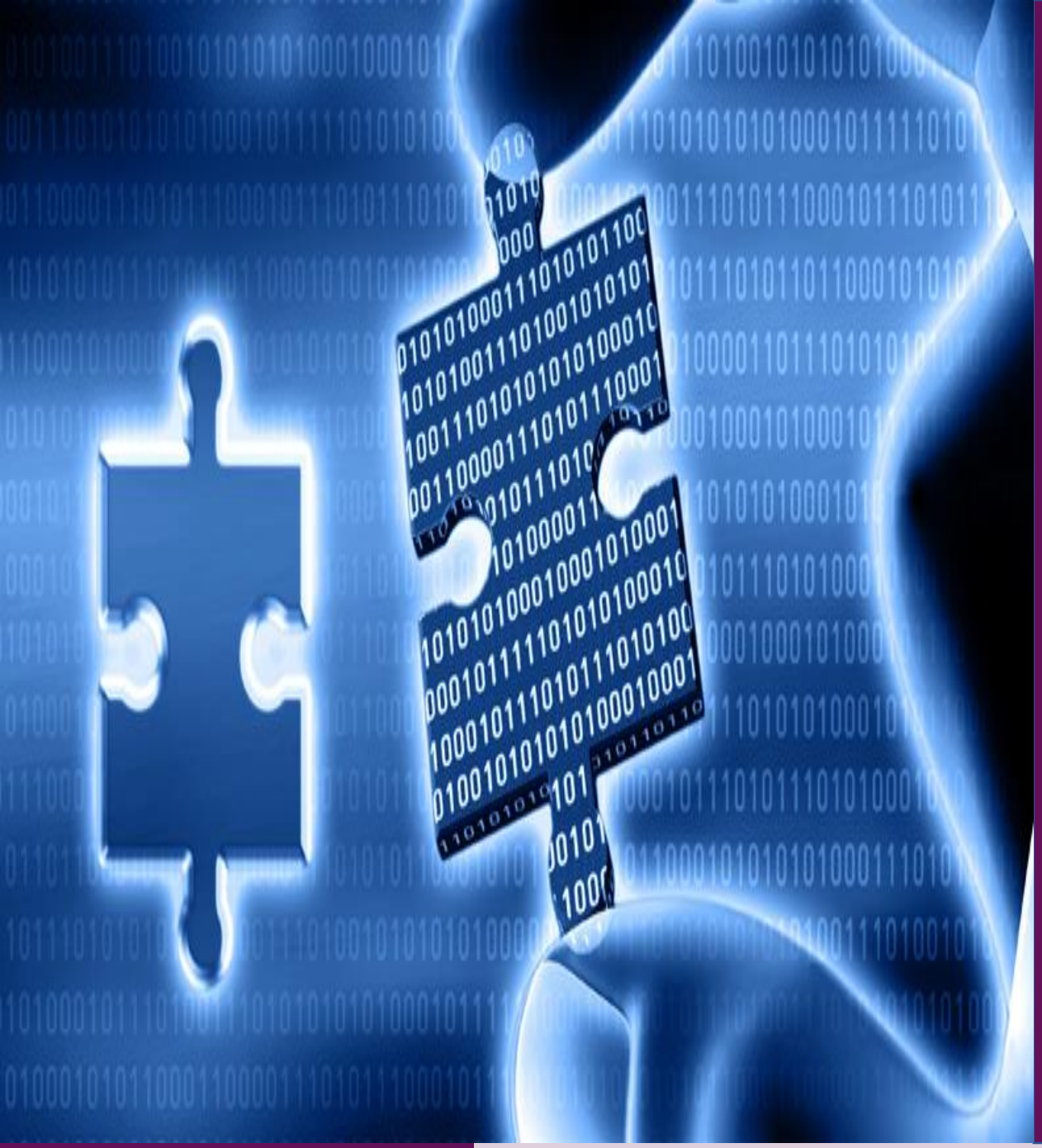
SCIENTIFIC STRUCTURE

6 research groups:

- **AMACC**: Algorithms, Computational Models, Combinatorial, Complexity,
- **CODAG:** Constraints, Ontologies, Data, Annotations, Graphs
- **MAD**: Models, Agents and Decisions
- **IMAGE**: Image processing and understanding
- **ELEC:** Electronics
- **SAFE:** Security, Architectures, Forensics, biomEtrics

PLAN

- GREYC research lab
- **Introduction to digital forensics**
- Expert in digital forensics
- G'DIP platform
- Tools illustrations
- Perspectives



Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

DIGITAL FORENSICS

Process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

DIGITAL FORENSICS STEPS

Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

1. Identification

First, find the evidence, noting where it is stored.

2. Preservation

Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

3. Analysis

Next, reconstruct fragments of data and draw conclusions based on the evidence found.

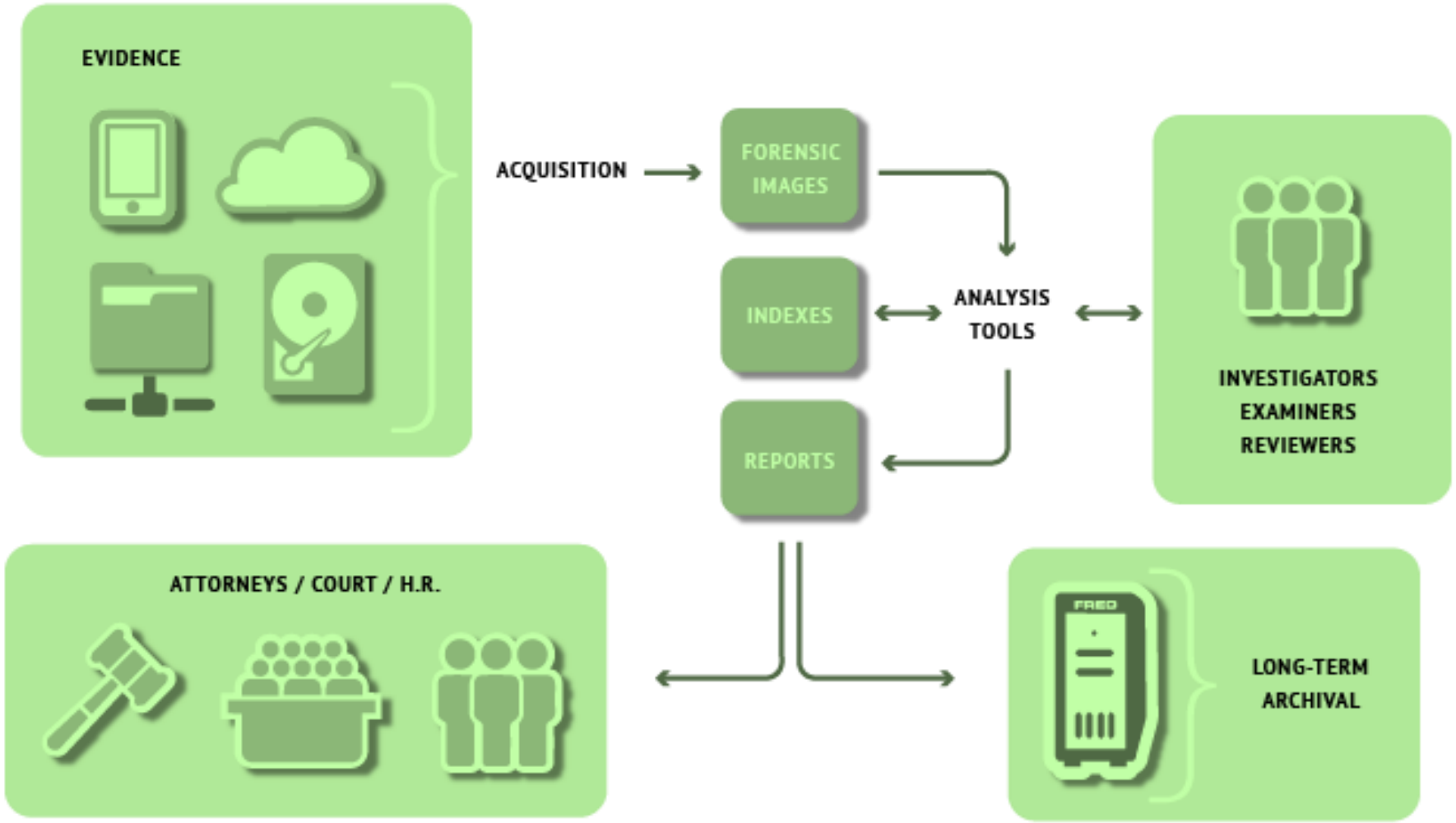
4. Documentation

Following that, create a record of all the data to recreate the crime scene.

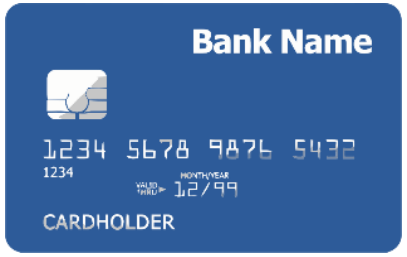
5. Presentation

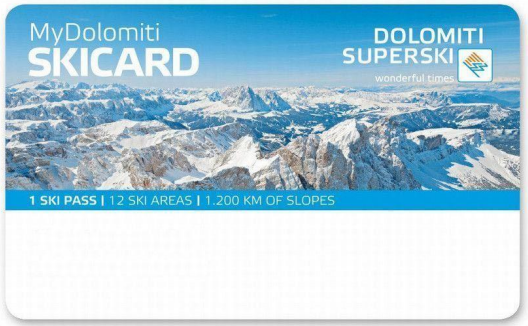
Lastly, summarize and draw a conclusion.

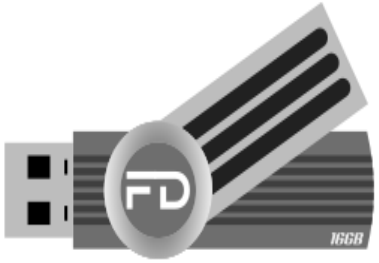
DIGITAL FORENSICS



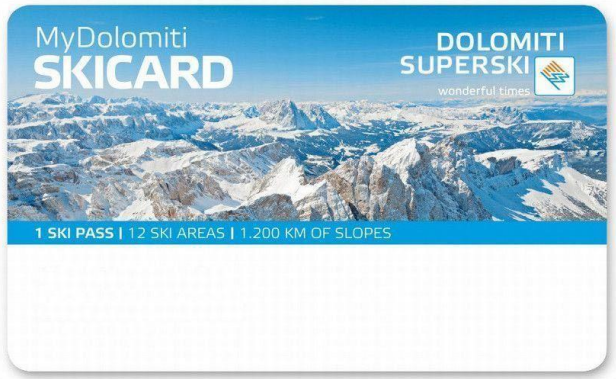
DIGITAL FORENSICS MEDIA

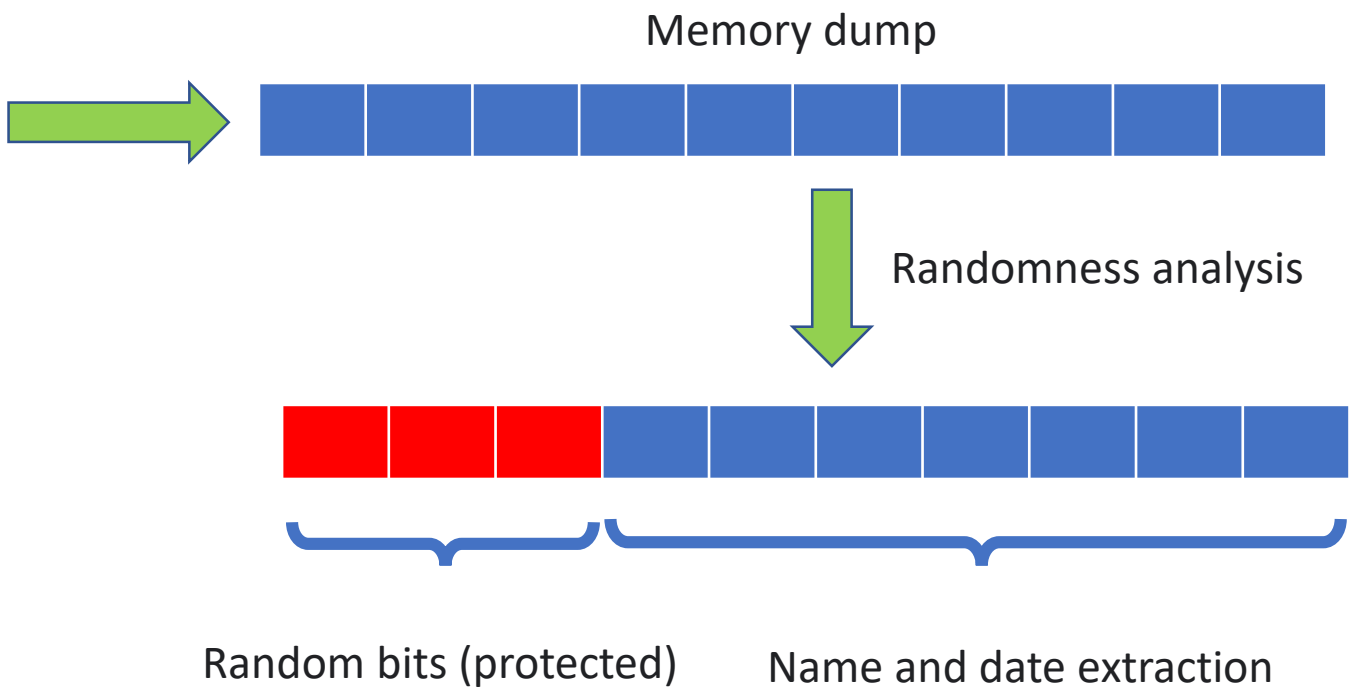






EXAMPLE: MEMORY DUMP ANALYSIS





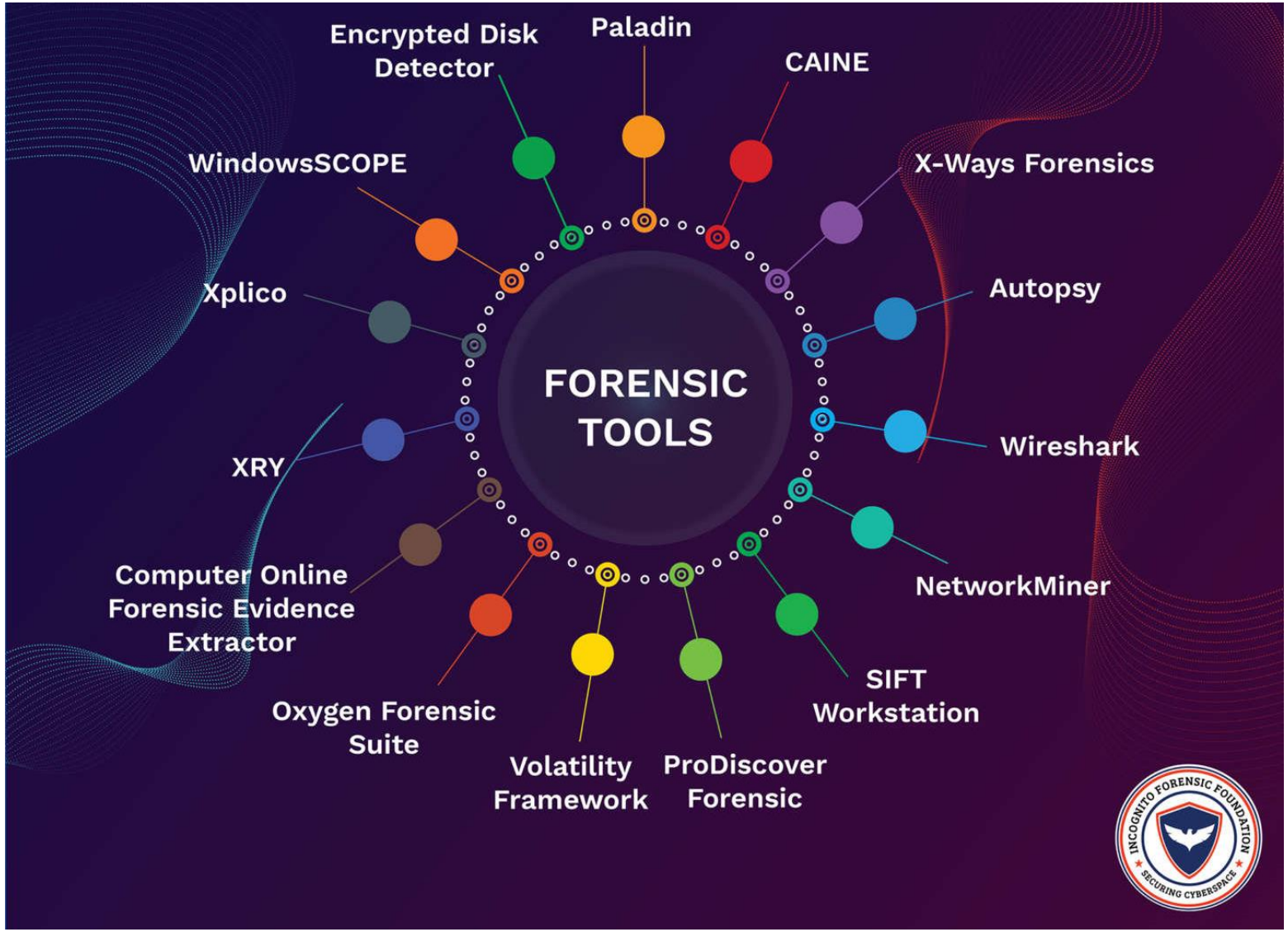
Applications:

- ❑ Privacy analysis
- ❑ Tool for the police forces

Gougeon, T., Barbier, M., Lacharme, P., Avoine, G., & Rosenberger, C. “Memory Carving in Embedded Devices : Separate the Wheat from the Chaff”. In International Conference on Applied Cryptography and Network Security (ACNS’16) (pp. 592-608). Guildford, United Kingdom.

Gougeon, T., Barbier, M., Lacharme, P., Avoine, G., & Rosenberger, C. “Memory carving can finally unveil your embedded personal data”. In International Conference on Availabity, Reliability and Security (ARES’17) (9 pages). Reggio Calabria, Italy.

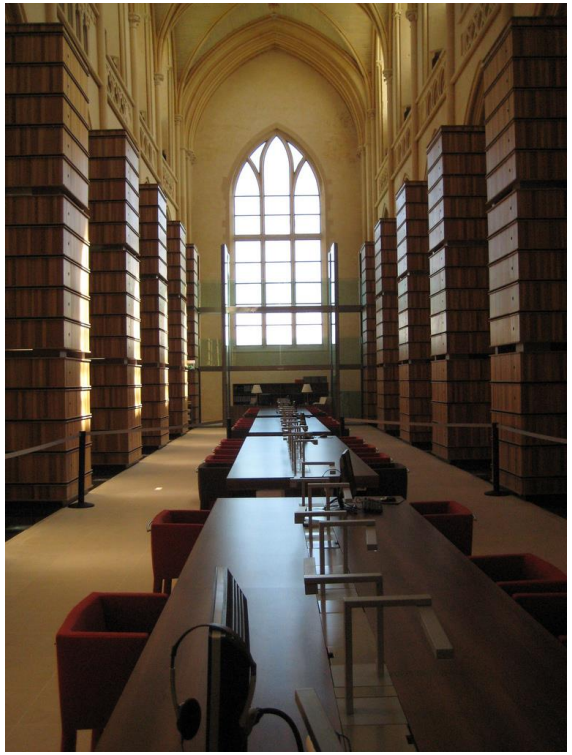
DIGITAL FORENSICS TOOLS



DIGITAL FORENSICS APPLICATIONS

- Analysis of crime evidence
- Missing person

- How personal data are protected?
- High level analysis (sentiment, geolocation
- Identifying users



- Culture heritage analysis from digital data

PLAN

- GREYC research lab
- Introduction to digital forensics
- **Expert in digital forensics**
- G'DIP platform
- Tools illustrations
- Perspectives

Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

FEEDBACK OF A DIGITAL FORENSIC EXPERT

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

PRELIMINARIES

- Legal Expert for a Regional Court of Appeal
- During 10 years from 2005 until 2015
- Average of 3 cases per year
- Independent expert
  - ✓ « Free »: no pressure, no advices from authorities
  - ✓ Reproducible Method: Forensically sound
  - ✓ Legally responsible (specific insurance)
  - ✓ Stay focus on the case and write facts

DIFFERENT CYBERCRIMES

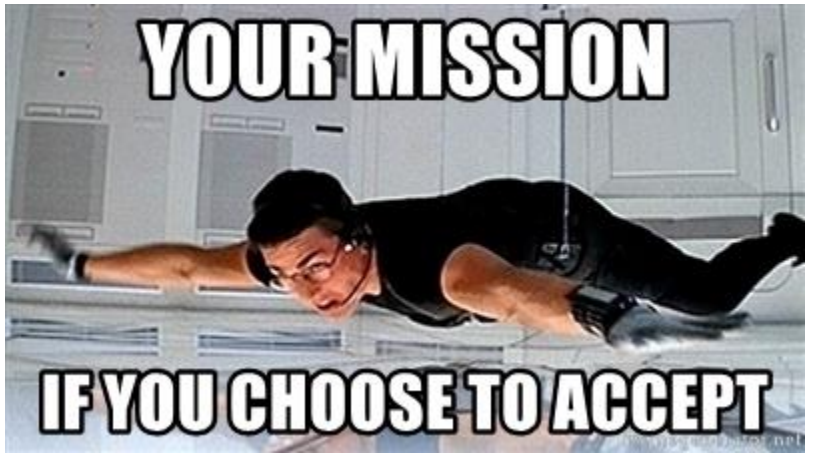
- Social fraud: forgery of official documents
- Trafficking in Intellectual Property
- Distribution and possession of child porn material
- Contacting children through the Internet
  - ✓ by sex predators/offenders or by "haters"
  - ✓ In order to get photos or videos
  - ✓ To meet the victim face to face
- Unconsented adult prostitution

LEGAL FRAMEWORK (1/2)

Origin of the requisitions:

- Security forces (National Police / Gendarmerie => law enforcement services)
- An Officer of the Judicial Police in charge of the investigation
- The regional public prosecutor
- A judge of the regional court

Accept or reject the mission ?



LEGAL FRAMEWORK (2/2)

In case of preliminary investigations:

- A complaint against someone
  - The investigation has started
  - During the search warrant, the Force has seized devices
- A search warrant given by a Court judge
  - Help the Forces to locate and seize the material
  - Start the digital investigation on site
- A suspect is placed in custody by Forces

  During 48 hours : suspicion of crime

ABOUT THE MISSION (1/2)

- Locate and Extract all information related to:
  - Possession and distribution of illicit content: copyrighted media / child porn / forgery
    Sort by category + Stats
  - Communication through Online Communication Services:
    Extract relevant excerpts and key information
    Nominative information (contact list): names, nicknames, logins, pseudos, …
    Places, Addresses, Phone Numbers...
- Two kind of targeted information:
  - Images (photos) and videos
  - Textual information
- To understand what happen:
  - Dive inside people's life : deep inside...
  - Hope to rapidly find traces, evidences…

ABOUT THE MISSION (2/2)

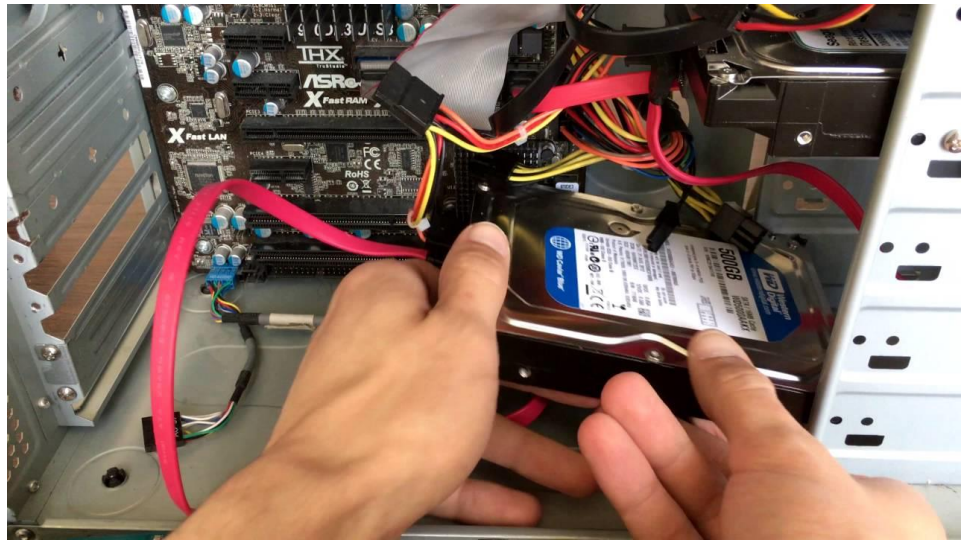
- Screen carefully the entire content (with an appropriate strategy) :
  - The visible part (expected and unexpected location, filenames)
  - The invisible part
- Achieve Multi-sources Analysis:
  - Computer Event Logs, Filetime Information, Web Browser Activity
  - Timestamped content => check/convert datetime
  - Media Content => Mail in Browser Cache, Attachment on FS
- Achieve Cross-device / Cross-computers Analysis:
  - Connected Devices: Run on a computer / Store in an external devices
  - Logs, Cache, Temp files / Content

THE PLAYGROUND (1/2)

- In a single case, several materials to handle:
  - 1 or 2 tower computers (incl. 1 or 2 internal disks : 250-500Gb each),
  - 2 laptops,
  - 1 or 2 external disks: 250-750Gb each
  - 2 or 3 USB Keys, 5 to 10 writable Cds or DVDs
- Analyze each device and Perform a Cross Analysis
  - Large quantity of information to handle: visible+recoverable
  - Time consuming process for a single person
  - Sources of errors and omissions are multiple

THE PLAYGROUND (2/2)

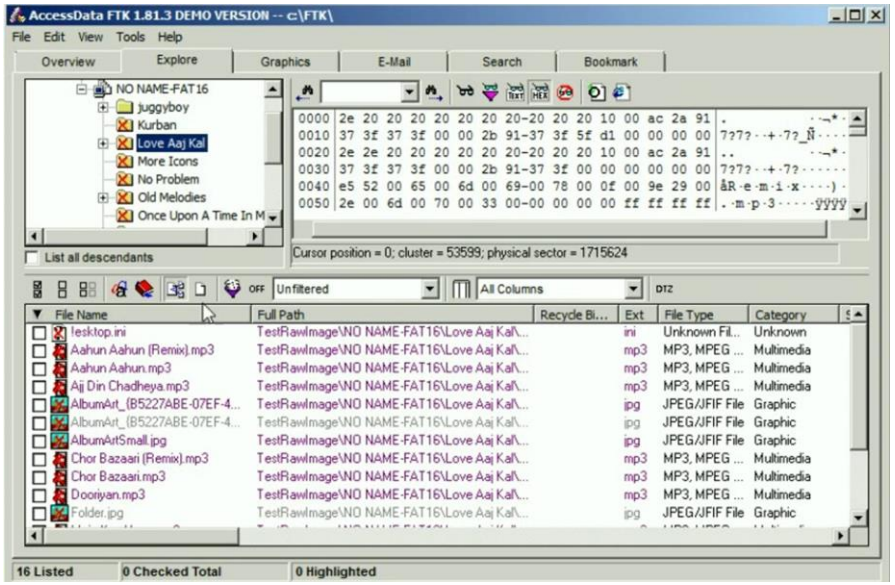
- The Materials in 2005-2015:
  - Mostly Tower Computers and Mobile Computers
  - Mostly Mechanical Disks
  - No disk encryption by default, or security by design
  - No mobile phones : analyzed by Forces with dedicated extraction devices (Cellebrite UFED)



- Internet Activities in 2005-2015:
  - Search Activity
  - Access to online services: Mail, Bank, Travel & Hotel Booking, Maps
  - Social Networks and Instant Messaging: various adhoc tchat platforms
  - Peer to peer (file sharing) activities
  - No cloud services except for Mail: various mail hosting platforms

TECHNOLOGICAL CONTEXT

- Digital investigation platforms:
  - EnCase, FTK, Autopsy, X-Ways, Magnet IEF/Axiom…
  - Extract traces and potential evidences
  - Manage the case
- Specific Forensic Tools:
  - Extract data from proprietary format (Security Exploded)
  - Recover deleted file / do File Carving
- Not always free, not open-source, not evaluated:
  - Am I missing something important ?



FORENSIC DATA ACQUISITION

- Follow forensically sound procedures
  - Original data has not been altered
  - Ensure that evidences will be accepted by the Court
- Software vs Hardware write blockers
  - Work in a safe environment
  - Disable OS automount or autorun / mount -ro
  - Set Disk Jumpers
  - Use professional Write blockers & Disk imagers

FORENSIC DATA ACQUISITION

- Forensically Sound Data Capture
  - Use Write blockers
  - Create disk image
  - Bit-by-bit copy with hashing on the fly (dcfldd, dc3dd)
- Limits
  - Disk stress
  - Time constraints

STARTING THE INVESTIGATIONS

- Discover disk structure
  - Check Partitioning : os, data, recovery, swap, ...
  - Discover Unallocated Space

STARTING THE INVESTIGATIONS

- Two strategies:
  - Examine via a terminal : sfdisk, mount
  - Boot the image in a virtual environment
- Mounting the image:
  - OS Name and version
  - Discover user accounts / Crack user passwords
  - Analyze with Forensic Tools & Forensic Platforms
- Boot the image:
  - Help diving in the case: Understand how the user works
  - Organization of the desktop, background image, shortcut icons
  - Help to rapidly get insights for easy cases / access distant content

DIGITAL FORENSIC ACTIVITIES

- Disk forensics
  - Including Web Browser Forensics
- Memory forensics
  - Passwords or hashes of passwords
  - Last activity
- Cloud forensics and Network forensics
  - Legal limit
- Encrypted content
  - Search applications
  - Locate containers
  - Ask credentials

DEALING WITH IDENTITIES

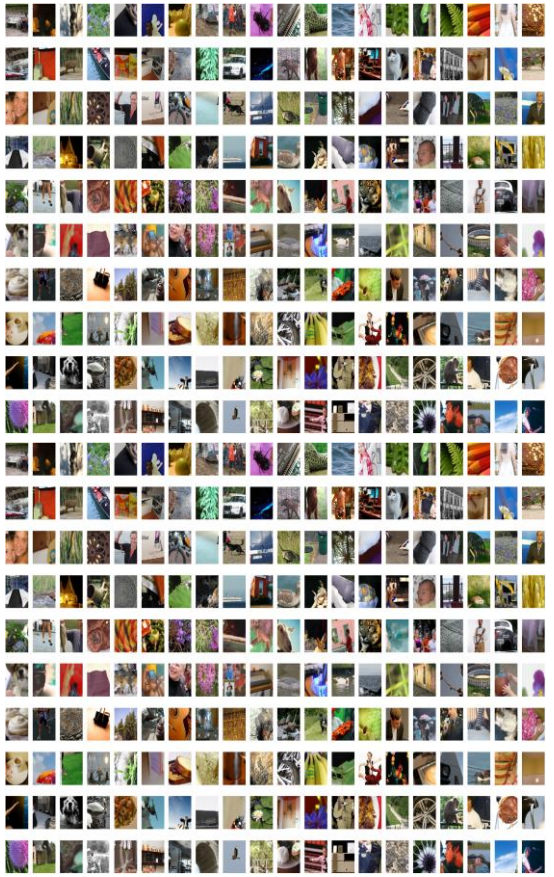
- Personal computers are shared
  - Often 1 shared account
  - Use of pseudos
- Linking Virtual and Real Identities
- Activity and Identity: Analysis of timeline
  - Reconstruction of timeline(s)
  - Detecting coherent/regular activity session
- « Written » Media Analysis (+OCR):
  - Reports, Letters, Invoices, eMails

DEALING WITH IMAGES (1/2)

- Dealing with tens of thousands of images per device
- The visible images (on the FS):
  - Photos (personal/downloaded)
  - Synthetic Images: Icons, software images
- The duplicates images:
  - Arise with File Carving & Cross device analysis
  - Filtering Techniques : Databases of hashes of positive or negative
- The near-duplicates images:
  - resized / cropped /multiple format
  - PhotoDNA

DEALING WITH IMAGES (2/2)

- Thumbnail Databases :
  - To Accelerate Preview of Folder Content (OS based),
  - Digital Image Managers and Editors, Video Players, Media Players
- Software Cache :
  - Web Browser Cache
  - Web Browser Forensics
- Lost images : File Carving Techniques
  - Deleted Files, Temporary files, Files in unallocated spaces



ISSUES WITH DEALING WITH IMAGES

- Filtering Techniques :
  - Databases of hashes of positive or negative
- The problem of duplicates or near duplicates:
  - Photos may be resized / cropped / edited / multiple format
  - PhotoDNA
- From EXIF metadata to content based analysis
  - Separate Photos from Synthetic Images
  - Authorship Attribution : Downloaded or Taken ? Group by camera model ?
  - Group by event: party, wedding, winter holidays,
  - Group by locations : indoor (in the same apartment), outdoor (garden, ...)
  - Face Gallery
  - Explicit content

DEALING WITH VIDEOS

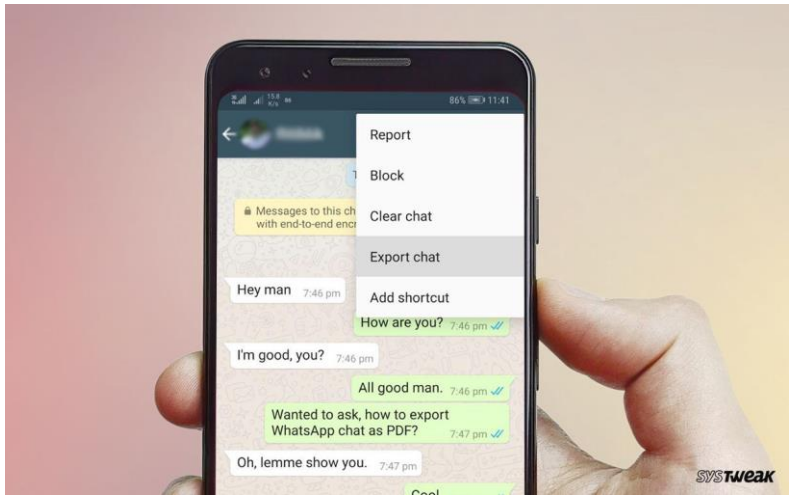
- High watching time
  - Extract a frame every 10 seconds
- Possible issues:
  - Select Key Frames
  - Segment in coherent scenes
  - Summarize

DEALING WITH TEXT

- Often seen as Keyword search but…
  - Image of document => OCR
  - Keyword search => Encoding / Language
  - Proprietary format => Extractor
  - Named Entities Recognition
- Online Conversation Reconstruction:
  - Protocol understanding (reverse engineering)
  - Locate received frames / sent frames (timestamped)

DEALING WITH CONVERSATIONS

- Online Conversation Mining:
  - Tons of short messages:
    - Refers to many contacts / Spread over hours/days/weeks
  - Handle specific language (abbreviations, smileys...)
  - Combine with device events (camera / mic.)
  - Identify Communication Pattern
  - Handle change of Online Conversation Services
  - Simultaneous usage of devices: Chat with a computer + Send a photo by phone + receive photo stored on an external disk



DIGITAL FORENSICS ISSUES

- Towards Forensics Labs ?
  - Initial Costs: Materials (computers, storage devices, write blockers, disk imagers, connectors)
  - Recurring Costs: Software licenses
- Improving Trust: Cooperation between Industrials and Academics
  - Need for more independent evaluations, more open source tools
  - Need to handle new technologies, usages, software, services, versions
- Know-how & Sovereignty issue (Palantir-like corp.) ?
  - Default encryption / Hardware Security Module
  - Computer forensics companies
- Towards IA Tools ?
  - Text: Restricted to Keyword Search, Regexp Search and Named Entities ?
  - Image/Video: Towards Content-Based Search & Falsification Detection

PLAN

- GREYC research lab
- Introduction to digital forensics
- Expert in digital forensics
- **G'DIP platform**
- Tools illustrations
- Perspectives

GREYC Digital Investigation Platform

GREYC
Electronics and Computer Science Laboratory

Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

G'DIP PLATFORM

An open-source platform for digital forensics with evaluated tools

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

MOTIVATIONS

Design of a software and hardware platform:

- Automation of the analysis of digital traces of heterogeneous data
- Media: files, text, image, Web, dumps, network packets, etc.
- Composed of evaluated tools with benchmarking

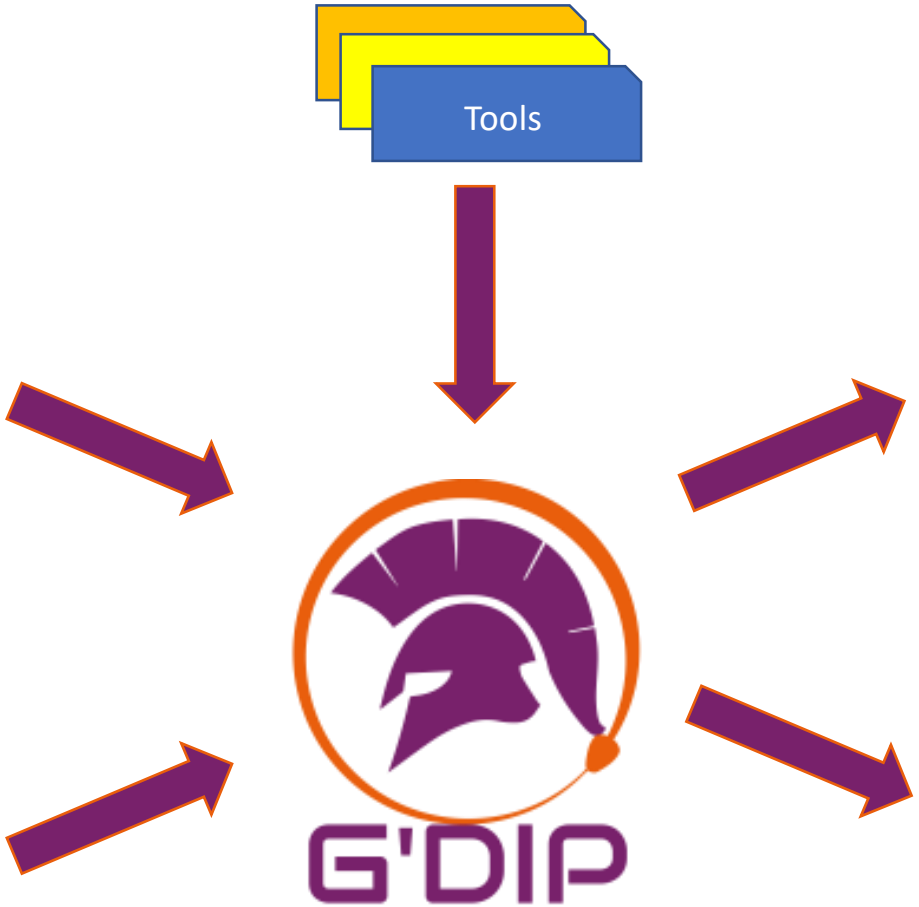
Research:

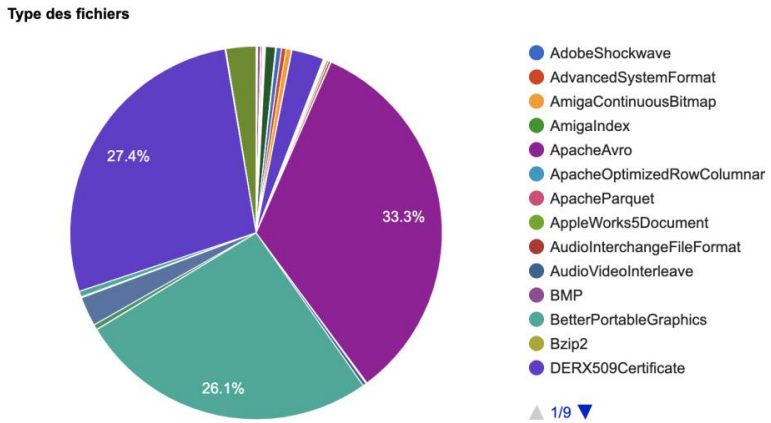
- Capitalize on GREYC research lab skills in natural language processing, image processing, machine learning, cryptography, network, smart card, randomness...
- Benchmark forensic tools: rigorous protocols, use of existing/new evaluation corpus
- Design of new forensic tools

Teaching:

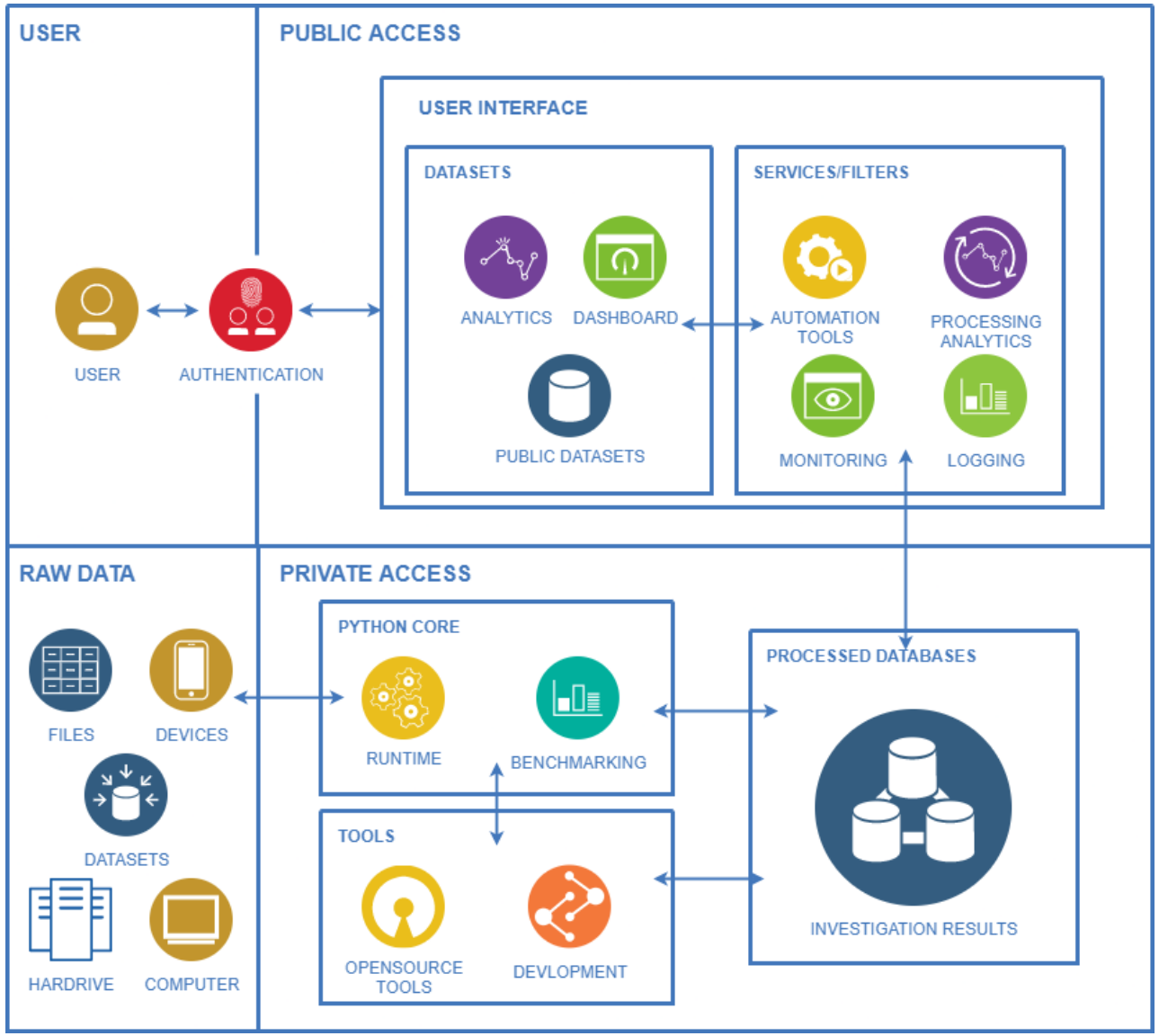
- Support of forensics lecture with practical works on the G'DIP platform
- Projects and internships for the design of new functionalities
- Capture the flag creation for scientific mediation

PLATFORM


Tools
G'DIP


Type des fichiers
27.4%
33.3%
26.1%
AdobeShockwave
AdvancedSystemFormat
AmigaContinuousBitmap
AmigaIndex
ApacheAvro
ApacheOptimizedRowColumnar
ApacheParquet
AppleWorks5Document
AudioInterchangeFileFormat
AudioVideoInterleave
BMP
BetterPortableGraphics
Bzip2
DERX509Certificate
1/9

PLATFORM


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

RESULTS DATABASE

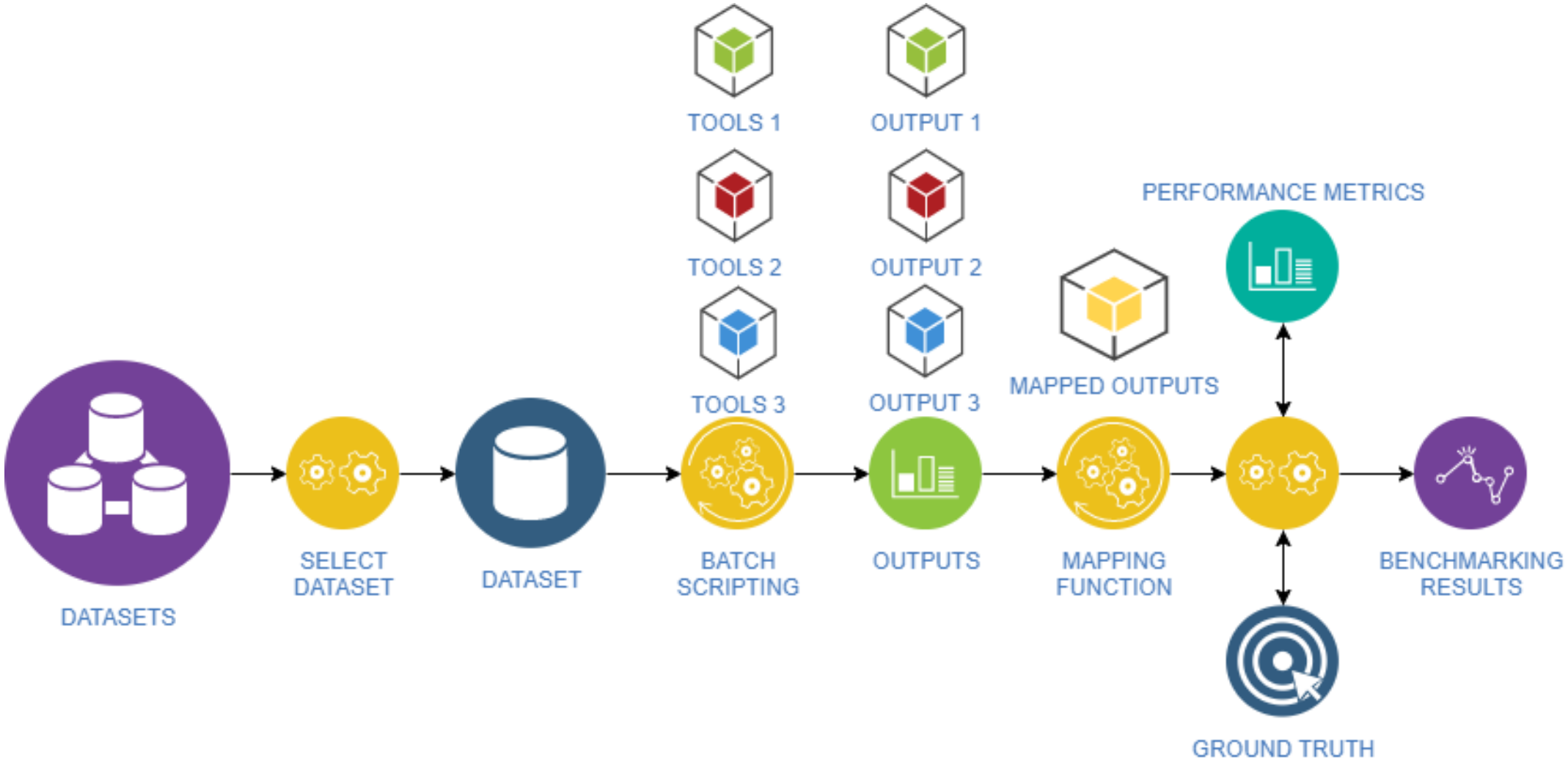
Basic file information

Tools results

id	name	directory	Creation date	Tool 1	Tool 2	Tool 3	Tool 4	Tool 5	Tool 6

Example of expected query: Show me images captured by user's smartphone in Normandy on December

BENCHMARKING METHODOLOGY



PLATFORM: HARDWARE

FRED Forensic Workstation from Digital Intelligence equipped with writing blocking systems

→ Preservation of media

PLATFORM: SOFTWARES, API

G'DIP PLATFORM

Distribution:

- ❑ Open-source
- ❑ Distribution with a signed convention

Perspectives:

- ❑ Designing a graphical user interface
  - ✓ Public use on small datasets for teaching, testing, scientific mediation
  - ✓ Private use (local installation) for investigation on real data
- ❑ Adding new tools based on resquests
- ❑ Discussion for a PhD thesis
- ❑ Publications

PLAN

- GREYC research lab
- Introduction to digital forensics
- Expert in digital forensics
- G'DIP platform
- **Tools illustrations**
- Perspectives

Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

ILLUSTRATIONS

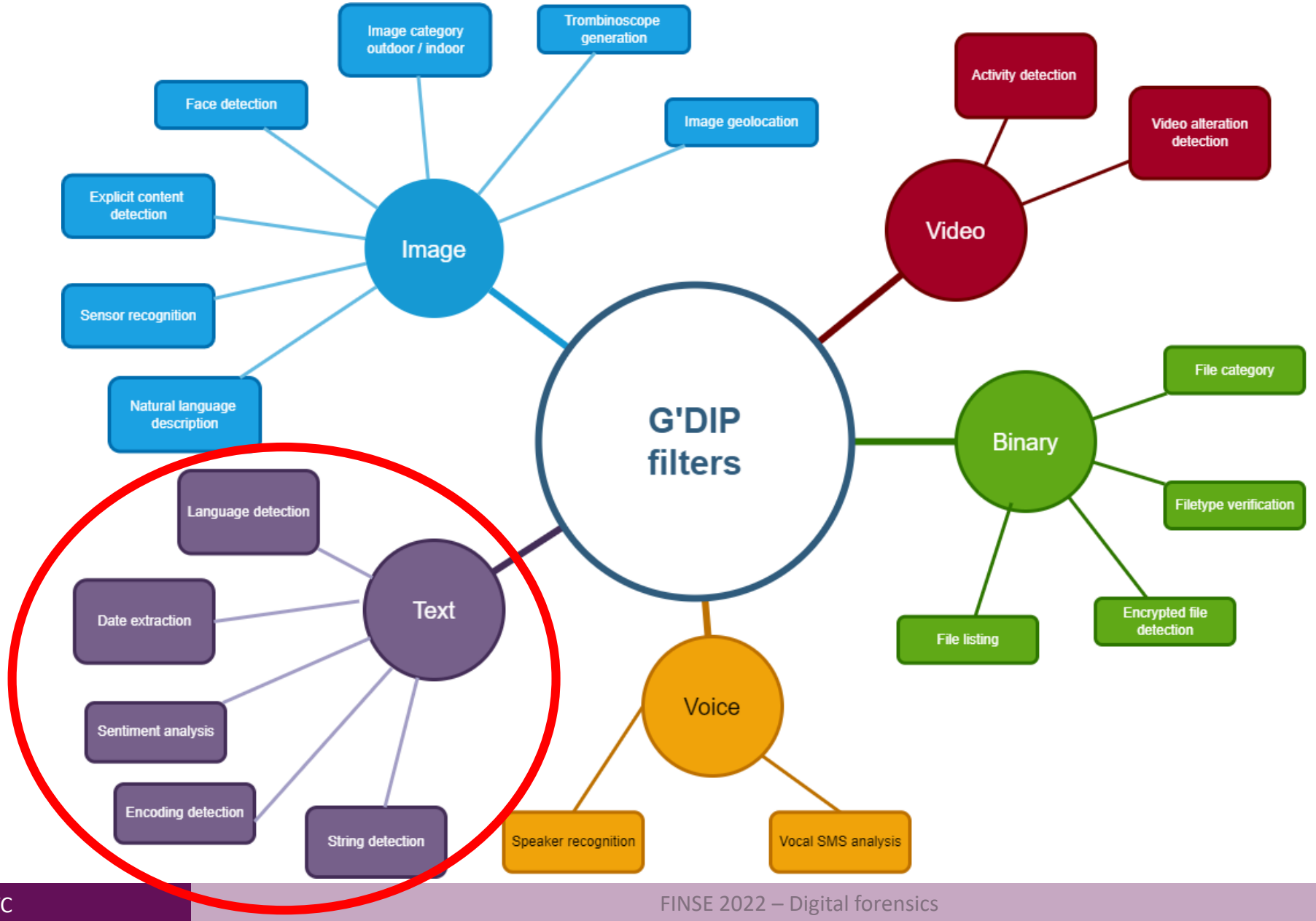
Building/using IA tools for analyzing digital traces

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

G'DIP FILTERS



BINARY – FILE LISTING

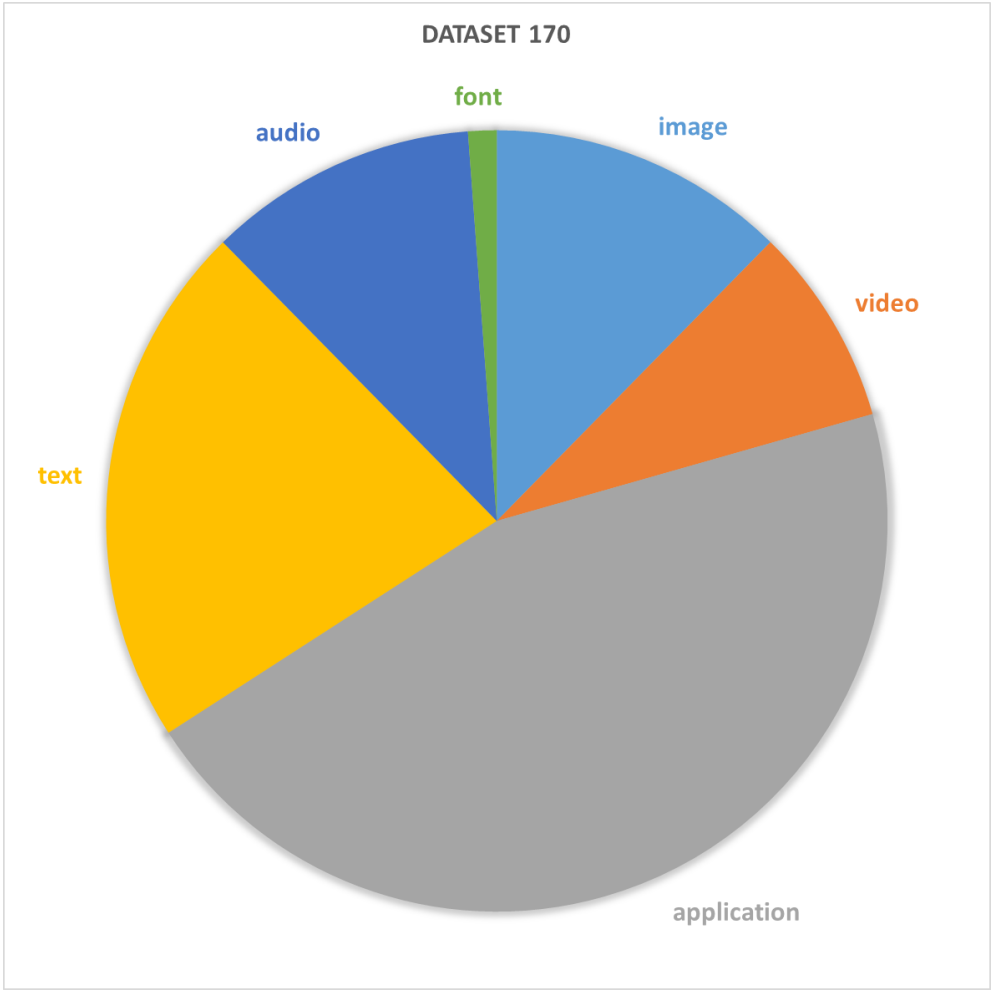
Objective: Listing all files in a directory/hard disk

file_id	name	extension	created_at	modified_at	size
5364	example	lz4	1616581245.2014892	1613818602	4
5365	example	lzfse	1616581245.2014892	1613818602	4
[illegible]	example	oar	1616581245.2014892	1613818602	3
5367	example	p25	1616581245.2014892	1613818602	4
5368	example	pbt	1616581245.2014892	1613818602	3
5369	example	pcv	1616581245.2014892	1613818602	4
5370	example	pgp	1616581245.2014892	1613818602	338
5371	example	rar	1616581245.2014892	1613818602	79
5372	example	rc	1616581245.2014892	1613818602	4
5373	example	rs	1616581245.217112	1613818602	8
5374	example	smi	1616581245.217112	1613818602	3
5375	example	stg	1616581245.217112	1613818602	4
5376	example.tar	xz	1616581245.217112	1613818602	6
5377	example.tar	z	1616581245.217112	1613818602	2

modified_at DATE

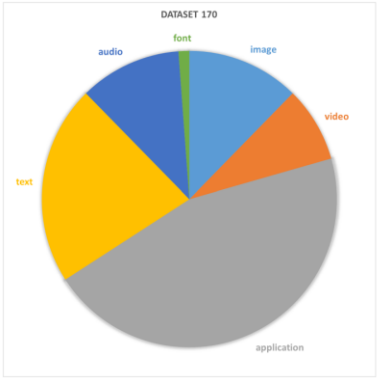
BINARY – FILE CATEGORY

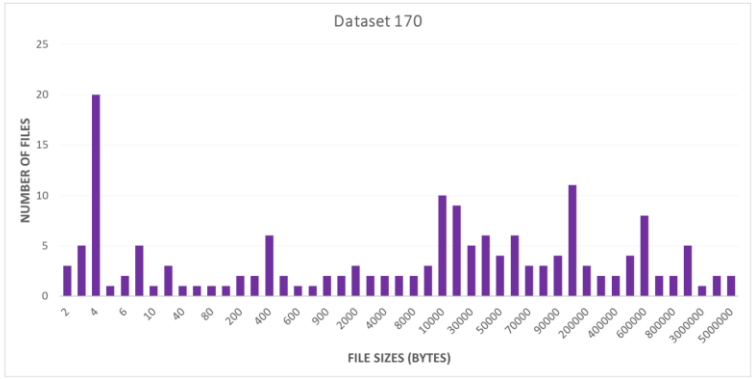
Objective: Classifying a file in different categories
Help the expert to focus on certain files

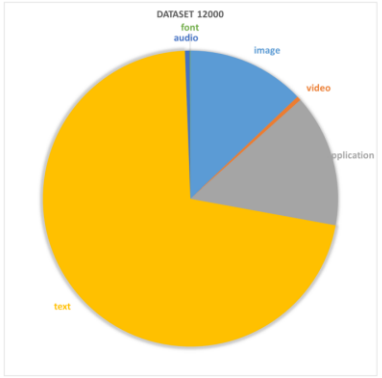


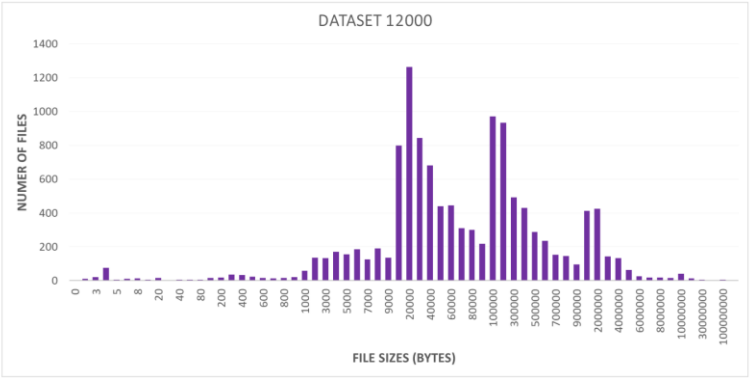
BINARY – FILETYPE VERIFICATION

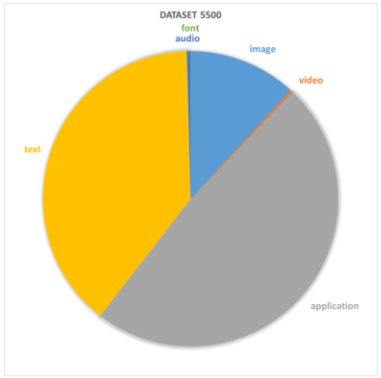
Objective: Has the filetype been modified?
Simple way to hide data on a computer (example: renaming a porn image to an exe file)

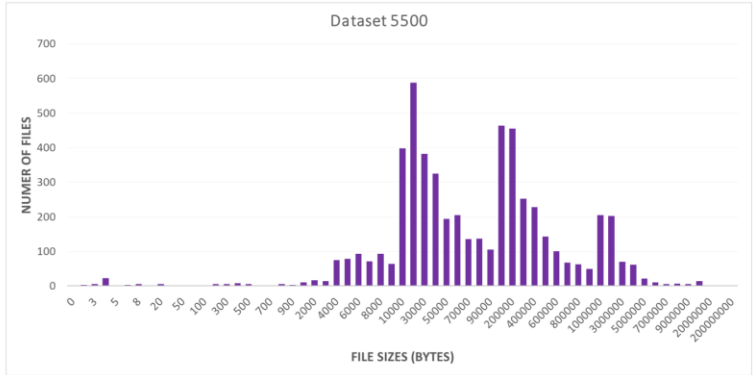












3 datasets:

- ❑ 170, 5500, 12000 files
- ❑ Maximising the different filetypes
- ❑ Ground truth

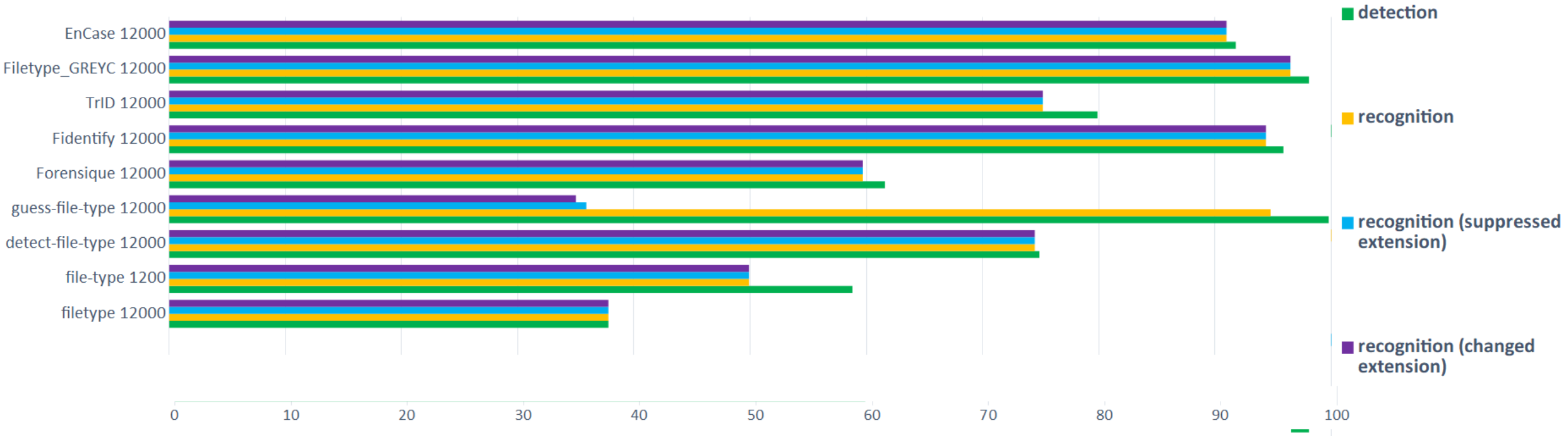
BINARY – FILETYPE VERIFICATION

Performance evaluation:

	Considered tools in the literature							
Datasets	***filetype***	***file-type***	***detect-file-type***	***guess-file-type***	***ForENSIque***	***Fidentify***	***TrID***	***EnCase***
170	101 - 59.4%	101 - 59.4%	99 - 58.2%	99 - 58.2%	**156 - 91.8%**	101 - 59.4%	147 - 86.6%	106 - 62.4%
5500	1917 - 34.9%	3283 - 59.7%	4161 - 75.7%	**5394 - 98.1%**	3346 - 59.460.8%	5328 - 96.9%	4372 - 79.5%	4740 - 86.2%
12000	4541 - 37.8%	4782 - 39.8%	6096 - 50.8%	7923 - 66%	7390 - 61.6%	**11534 - 96.1%**	9583 - 79.9%	11015 - 91.8%
Digital Corpora	426951 - 43.29%	648769 - 65.78%	791249 - 80%	376534 - 38.18%	648836 - 65.79%	967075 - 98.05%	827677 - 83.92%	not evaluated

	Considered tools in the literature							
Datasets	***filetype***	***file-type***	***detect-file-type***	***guess-file-type***	***ForENSIque***	***Fidentify***	***TrID***	***EnCase***
170	62ms	190ms	29ms	2852ms	376ms	227ms	11000ms	9000ms
5500	548ms	2099ms	519ms	98400ms	9685ms	28610ms	444000ms	14000ms
12000	1033ms	4782ms	1055ms	235000ms	21343ms	55415ms	894000ms	30000ms
Digital Corpora	4h40m15s	5h32m18s	3h44m42s	4h51m24s	6h40m53s	6h04m47s	17h55m15s	not evaluated

BINARY – FILETYPE VERIFICATION

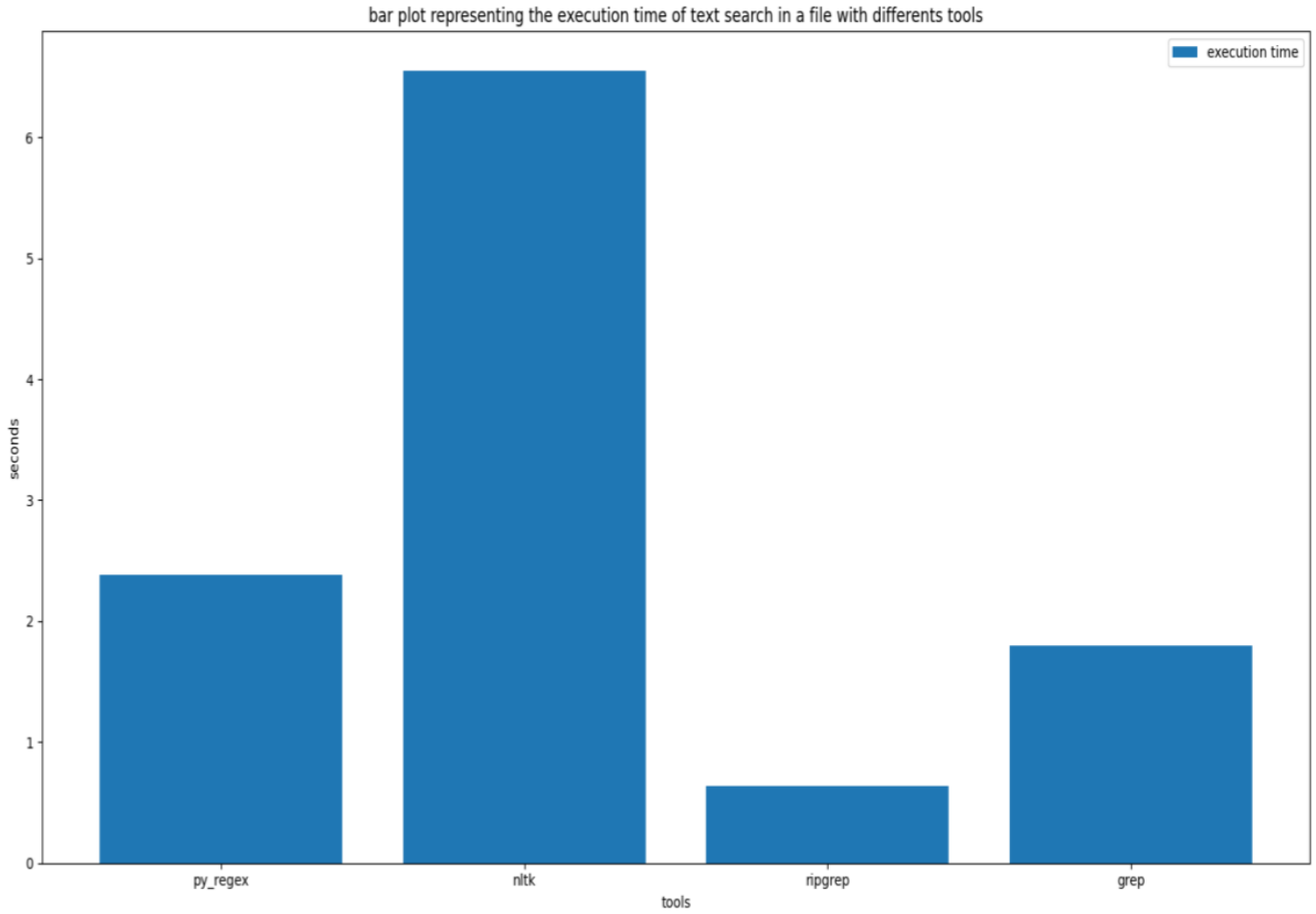


Conclusions (Dataset 12000):

- ❑ Some existing solutions provide poor results (file-type, guess-file-type..)
- ❑ Commercial solutions (EnCase, TrID) do not provide the best results
- ❑ Fidentify (open-source solution) provides good results
- ❑ Combing tools (Fidentify + Forensique) can achieve very good results (**98.5%** recognition rate)

TEXT – STRING DETECTION

Objective: File detection containing a specific string



Comparative study of existing libraries:

- ❑ Time computation
- ❑ Relative comparison

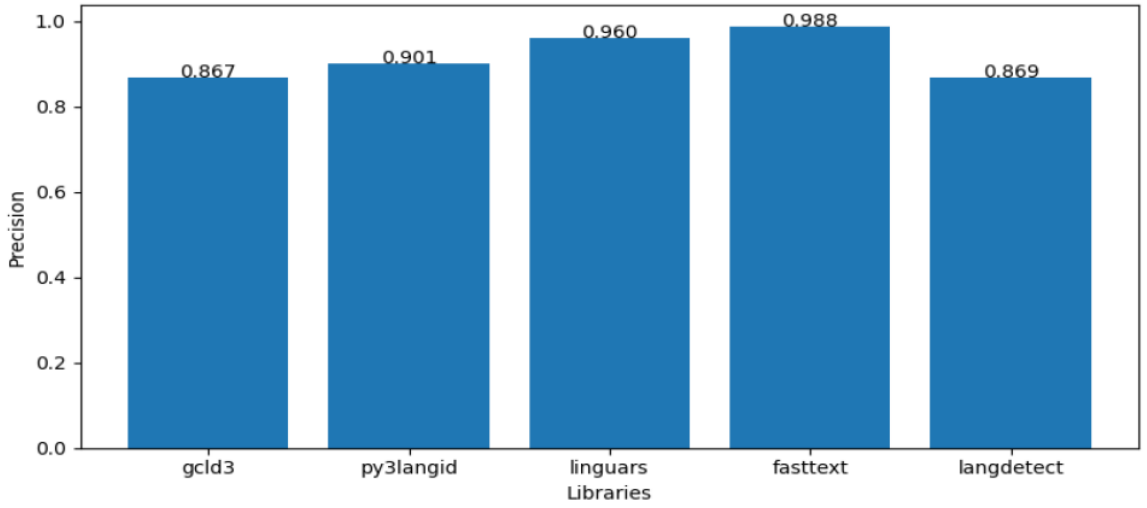
Perspectives:

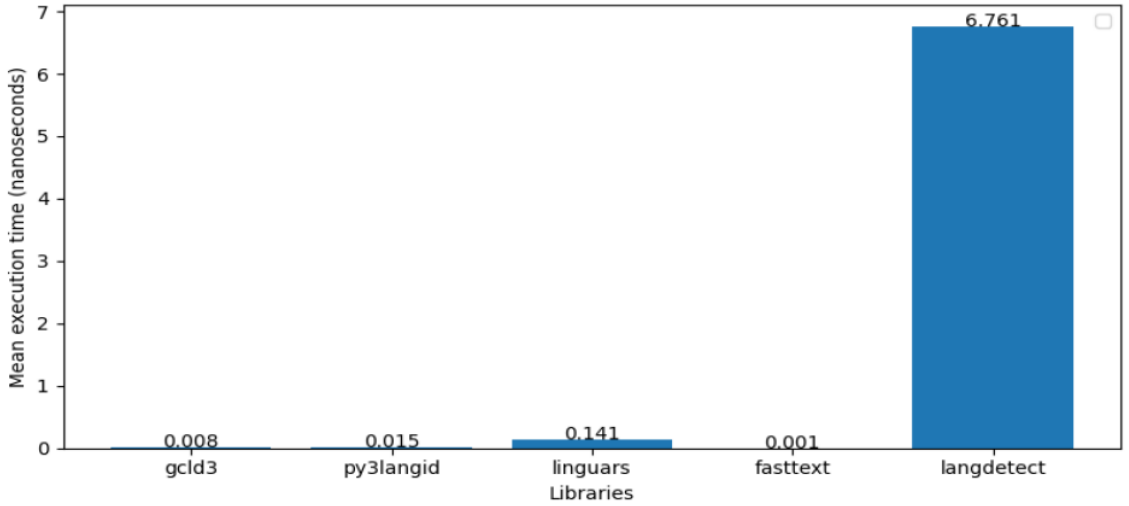
- ❑ Encoding detection
- ❑ Text extraction from documents (PDF…) as preprocessing (Apache TiKa)

TEXT – LANGUAGE DETECTION

Objective: Language detection in a text file
Dataset containing the 48 most known languages and about 8 Million sentences.
Each sentence is about 35 characters long and contains about 6 words.

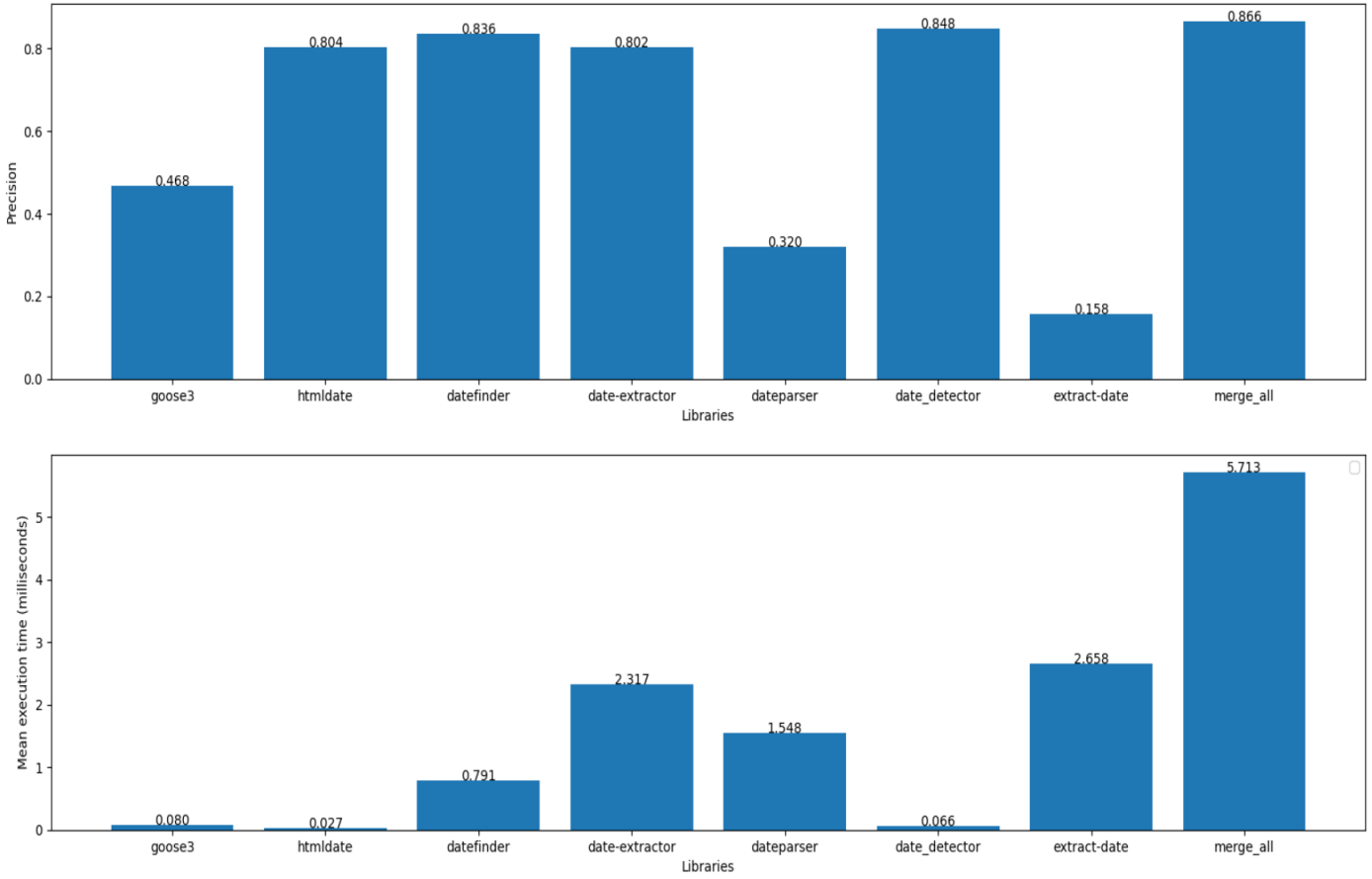
99.8% correct recognition with the Fasttext library with the lowest computation time





TEXT – DATE EXTRACTION

Objective: Date extraction in a text file
It could be useful for investigation (appointment, specific event)



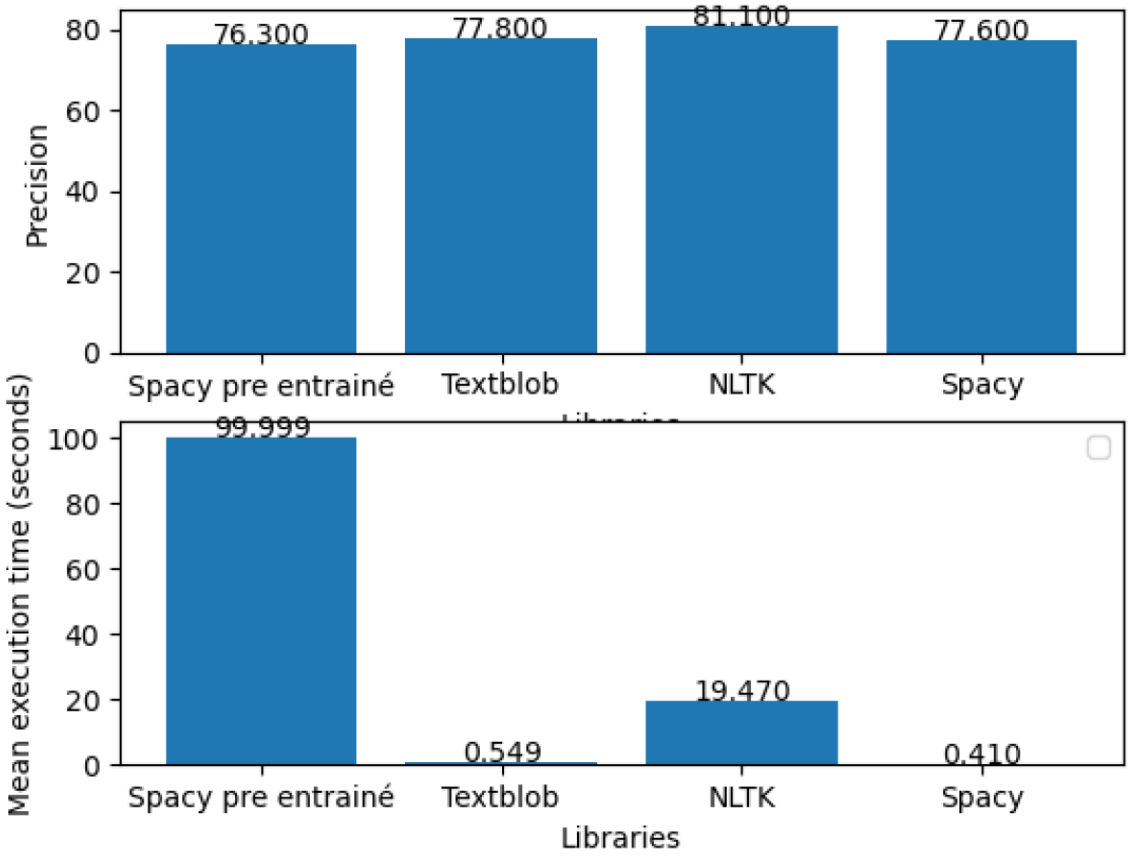
Comparative study of existing libraries:

- ❑ Dataset composed of 500 HTML files (with 40000 characters)
- ❑ Time computation
- ❑ Relative comparison

84.8% correct recognition with Date_detector library with low computation time

TEXT – SENTIMENT ANALYSIS

Objective: analyzing a text file to discover the sentiment hidden within it
Negative/positive content



Comparative study of existing libraries:

- ❑ Dataset composed of 2000 text files containing film critics
- ❑ Time computation
- ❑ Relative comparison

77.6% correct recognition with Spacy library with low computation time

Perspectives:
More sentiments (angry..)

G'DIP FILTERS

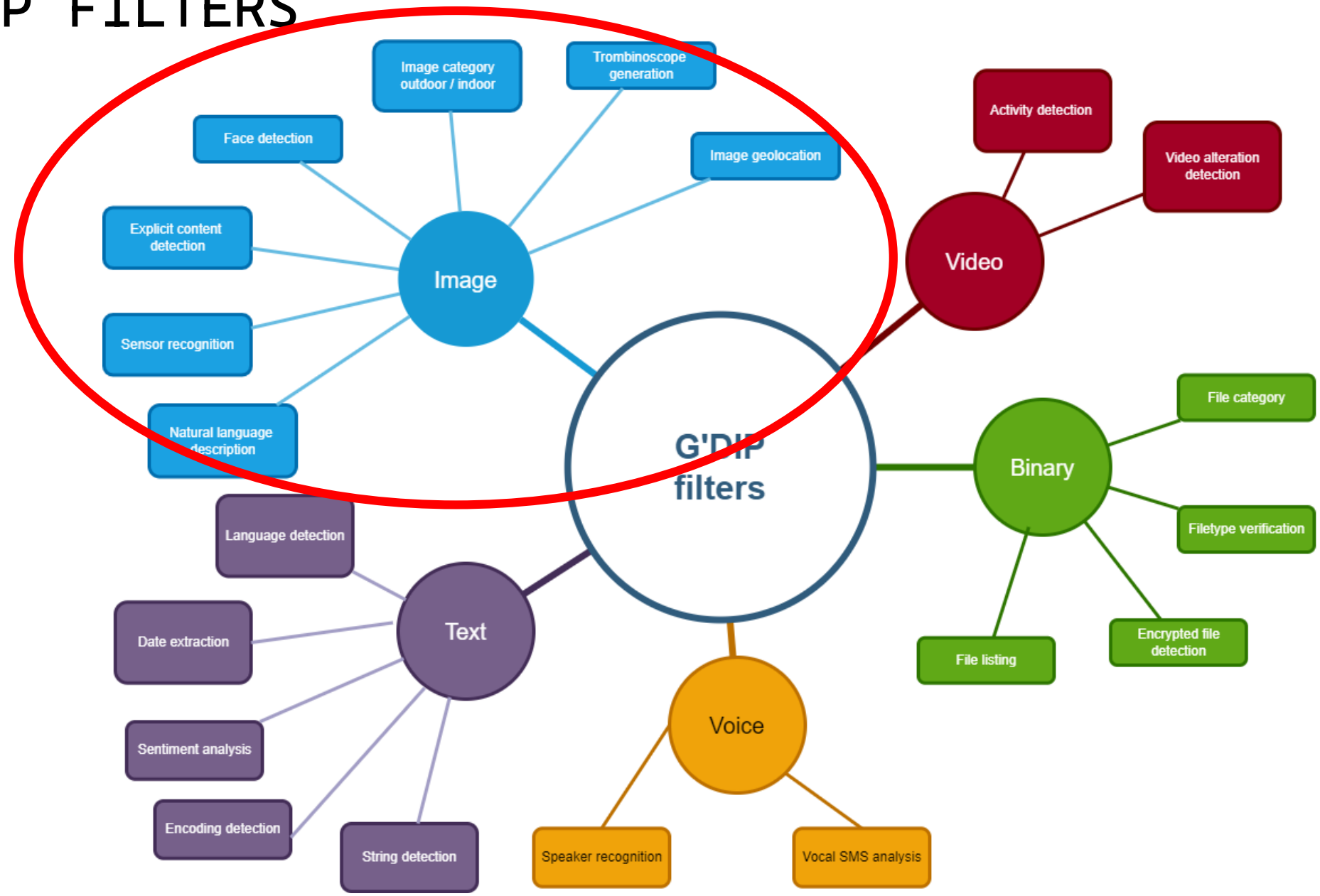


IMAGE – GENERAL PROCESS

Transfer learning for new tasks: adaption of paramaters for a new recognition task

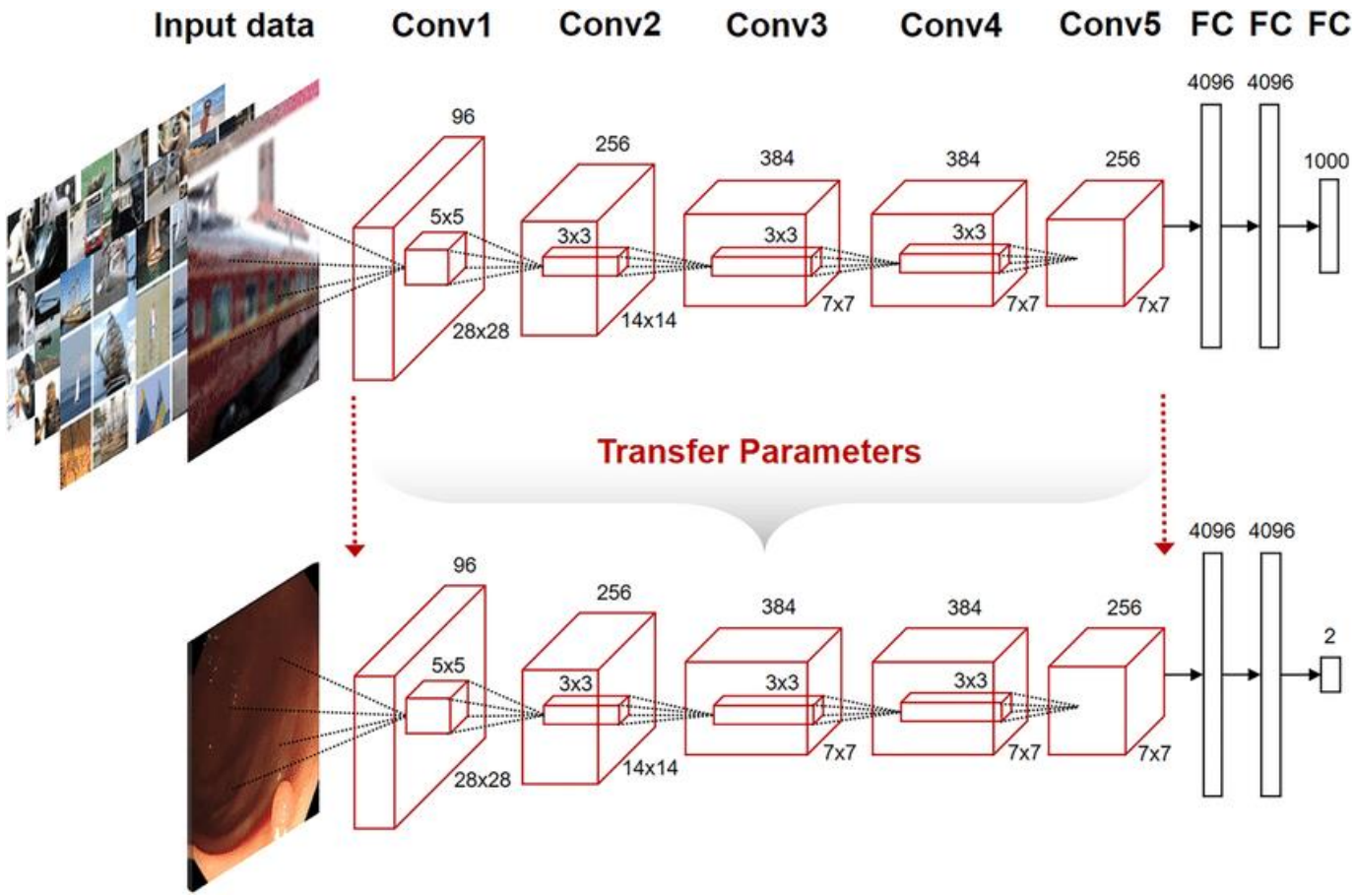


IMAGE – OUTDOOR/INDOOR

Objective: Does the image contain an outdoor/indoor scene?
A way to focus on certain types of images

MIT dataset:
- ❑ 2400 outdoor images
- ❑ 2400 indoor images

Transfer learning:
VGG 16 CNN

	precision	recall	f1-score	support
indoor	0.97	1.00	0.99	100
outdoor	1.00	0.97	0.98	100
accuracy			0.98	200
macro avg	0.99	0.98	0.98	200
weighted avg	0.99	0.98	0.98	200

→ outdoor

Easy task: 99% recognition rate

IMAGE – FACE PRESENT

Objective: Is there a face in the image?
Allows to filter images to analyze

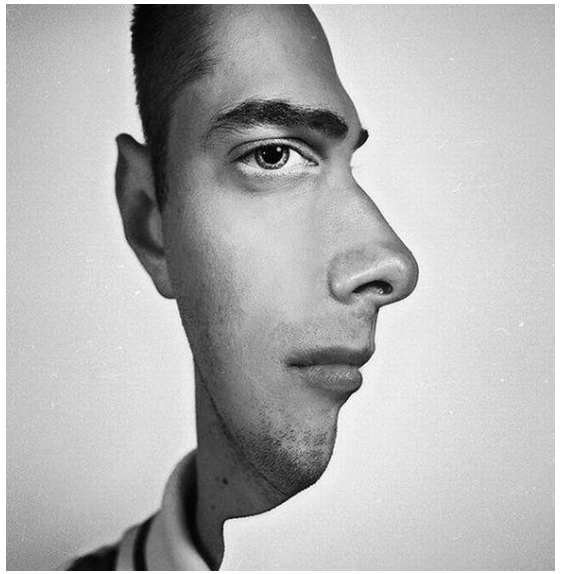
CALTECH 256 dataset

Transfer learning:
VGG 16 CNN

```
[INFO] evaluating...
              precision    recall  f1-score   support

        face       1.00      0.99      1.00       500
      noface       0.99      1.00      1.00       500

    accuracy                           1.00      1000
   macro avg       1.00      1.00      1.00      1000
weighted avg       1.00      1.00      1.00      1000
```



Face present

Easy task: 99% recognition rate

IMAGE – SENSOR RECOGNITION

Objective: Which sensor has been used to capture the image?
Did the suspected user capture an image?
Information on his/her geolocation at a specific date

Socrates dataset:

- ❑ 103 sensors
- ❑ 9700 images and 1000 videos

Transfer learning:
VGG 16 CNN

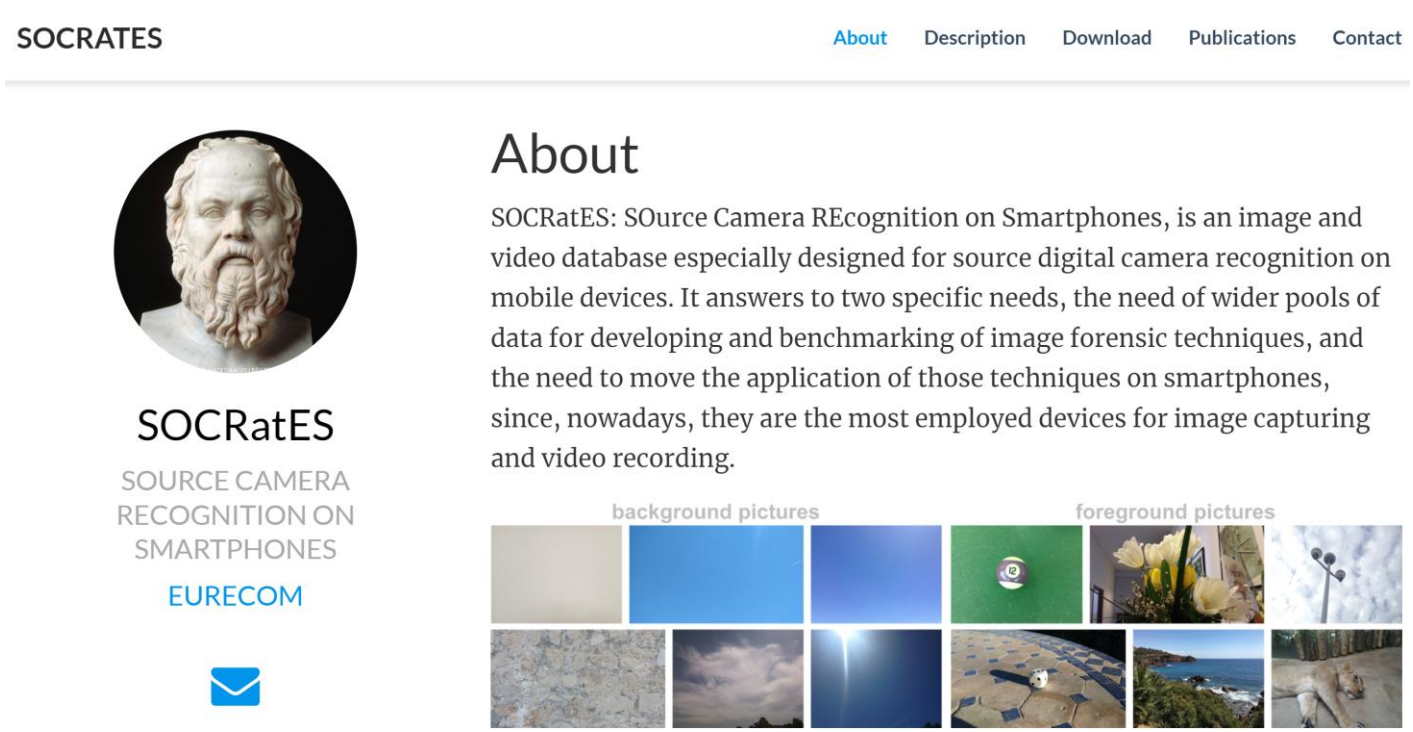
→ Apple Iphone 6

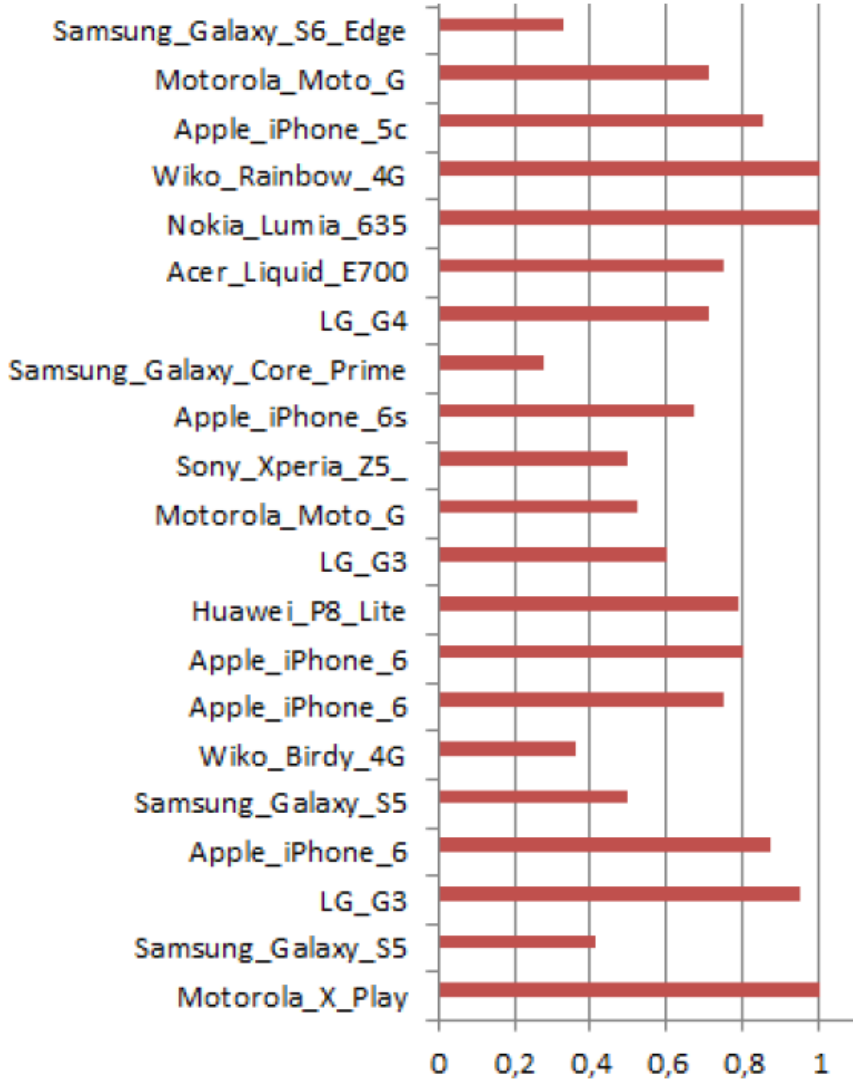
http://socrates.eurecom.fr/

IMAGE – SENSOR RECOGNITION

Experimental results:

- ❑ **66%** of recognition rate (in progress)
- ❑ Some sensors are easy to identify





Recognition rate [0,1]

IMAGE – EXPLICIT CONTENT DETECTION

Objective: Does the image contain an explicit content?
A way to focus on certain types of images

Dataset: training set composed of 650 000 files

nsfw_classifier		predicted classes	
		safe	*unsafe*
actual classes	*safe*	84%	16%
	unsafe	18%	82%

nudenet		predicted classes	
		safe	*unsafe*
actual classes	*safe*	87%	13%
	unsafe	20%	80%

Safe 82%

Quite easy task: 83% recognition rate

IMAGE – GEOLOCATION FROM CONTENT

Objective: where has been captured the image given its content?
Trace the geographical movements of a person

Model: LocationNet

- ❑ Transfer learning from GoogleNet
- ❑ https://aws.amazon.com/blogs/machine-learning/estimating-the-location-of-images-using-mxnet-and-multimedia-commons-dataset-on-aws-ec2/

Dataset:

- ❑ testing set composed of 3 000 files
- ❑ 10 images from 15 cities

Caen – France
GPS location: 49.18709, -0.35252

IMAGE – GEOLOCATION FROM CONTENT

Results:

- Very efficient in Europe and North America
- **86%** correct recognition (distance < 10km) for cities in Europe
- **80%** correct recognition (distance < 10km) for cities in France

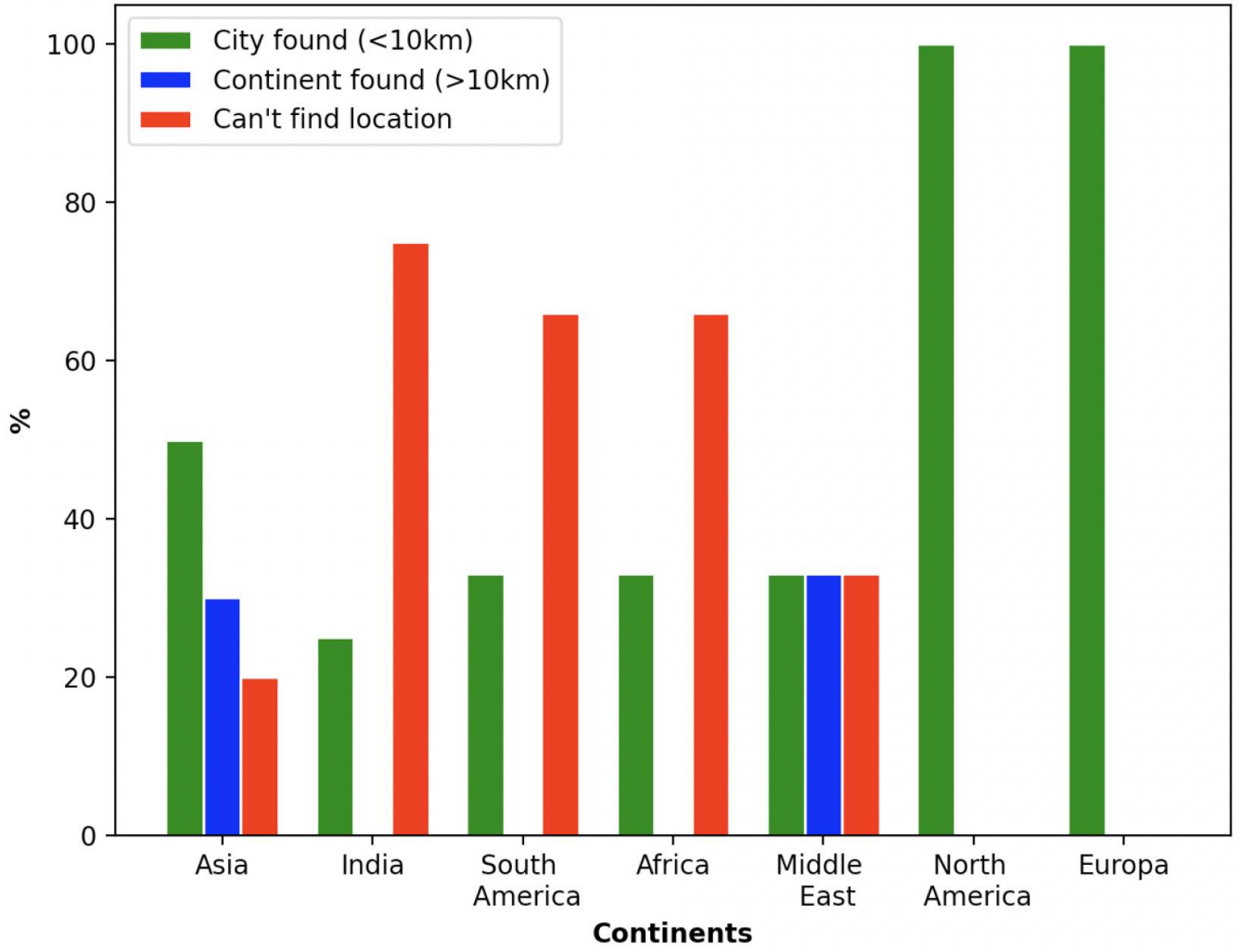


IMAGE – CAPTIONNING (IN PROGRESS)

Model: SSD: Single Shot MultiBox Detector

- Transfer learning from VGG 16
- https://github.com/weiliu89/caffe/tree/ssd
- Image description by counting some objects of interest (humans…)

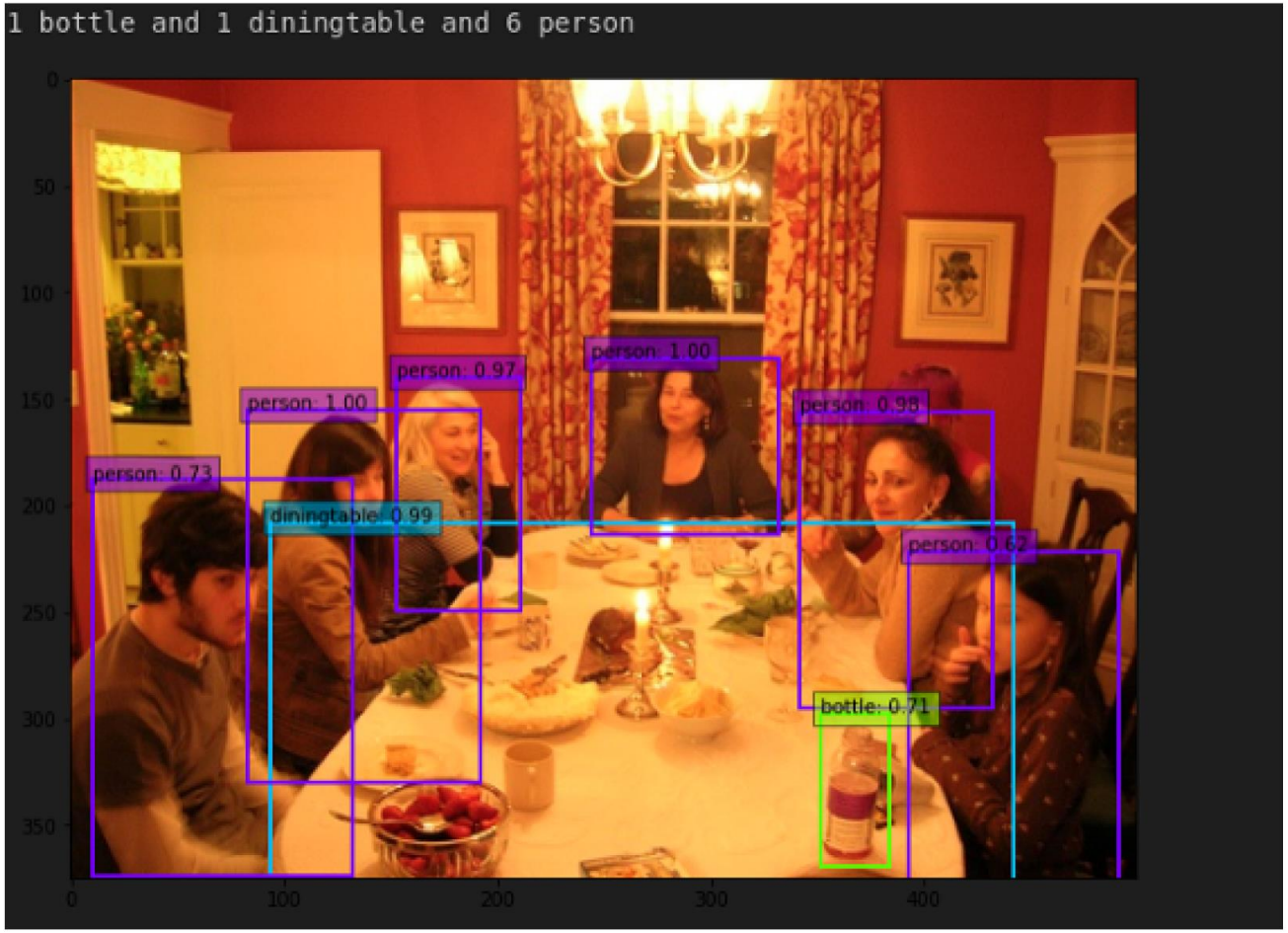


IMAGE – CAPTIONNING (IN PROGRESS)

Objective: Describing the content of an image
Text query on images

Model: IM2TXT

- Transfer learning from Inception V3
- https://github.com/HughKu/Im2txt
- 3 possible captions given an image

0) a tall clock tower with a sky background (p=0.002517)

1) a tall clock tower with a sky in the background (p=0.001261)

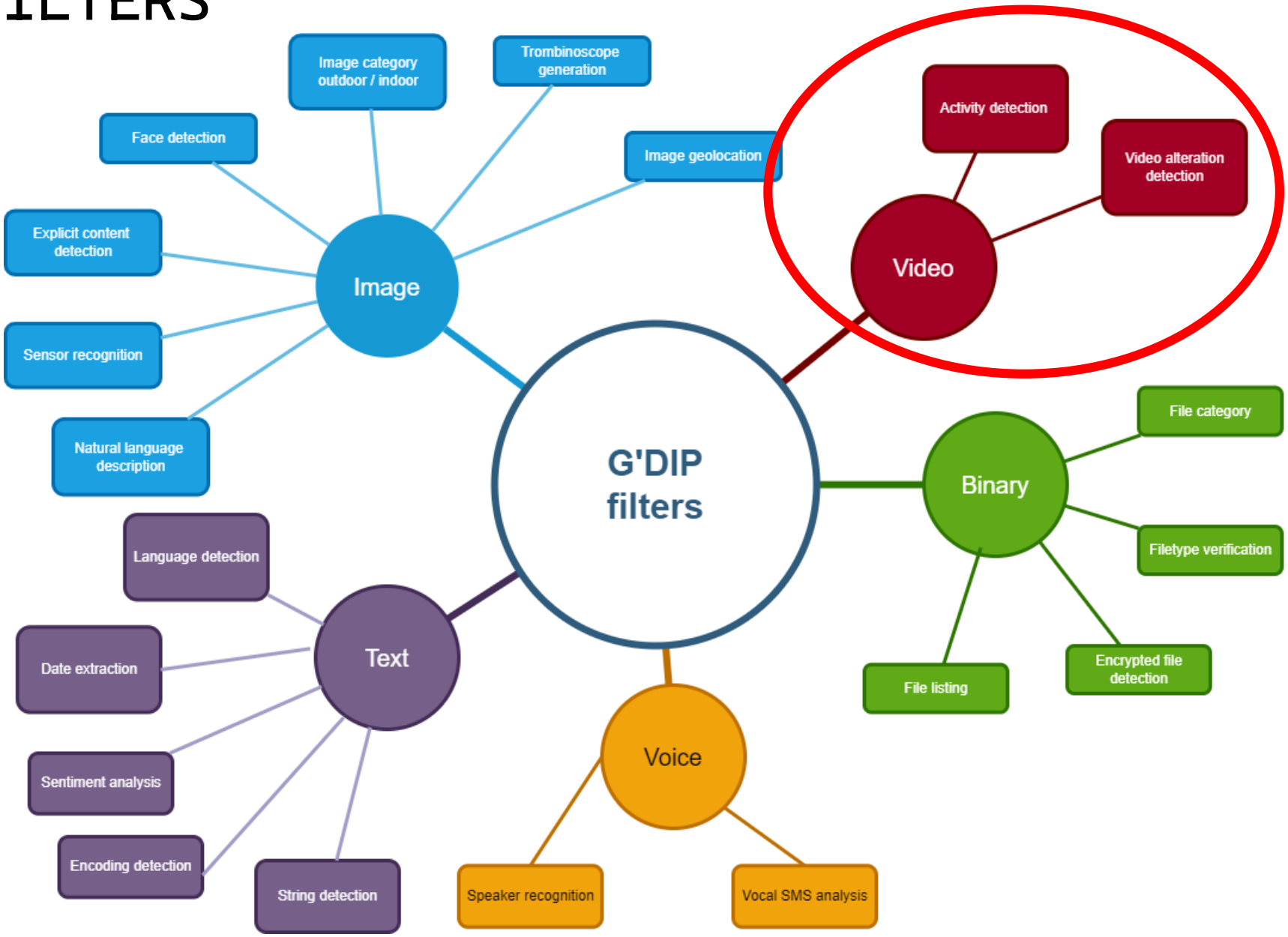
2) a tall clock tower with trees in the background (p=0.000807)

IMAGE – HUMAN DETECTION

Objective: Is there any human in the image ?

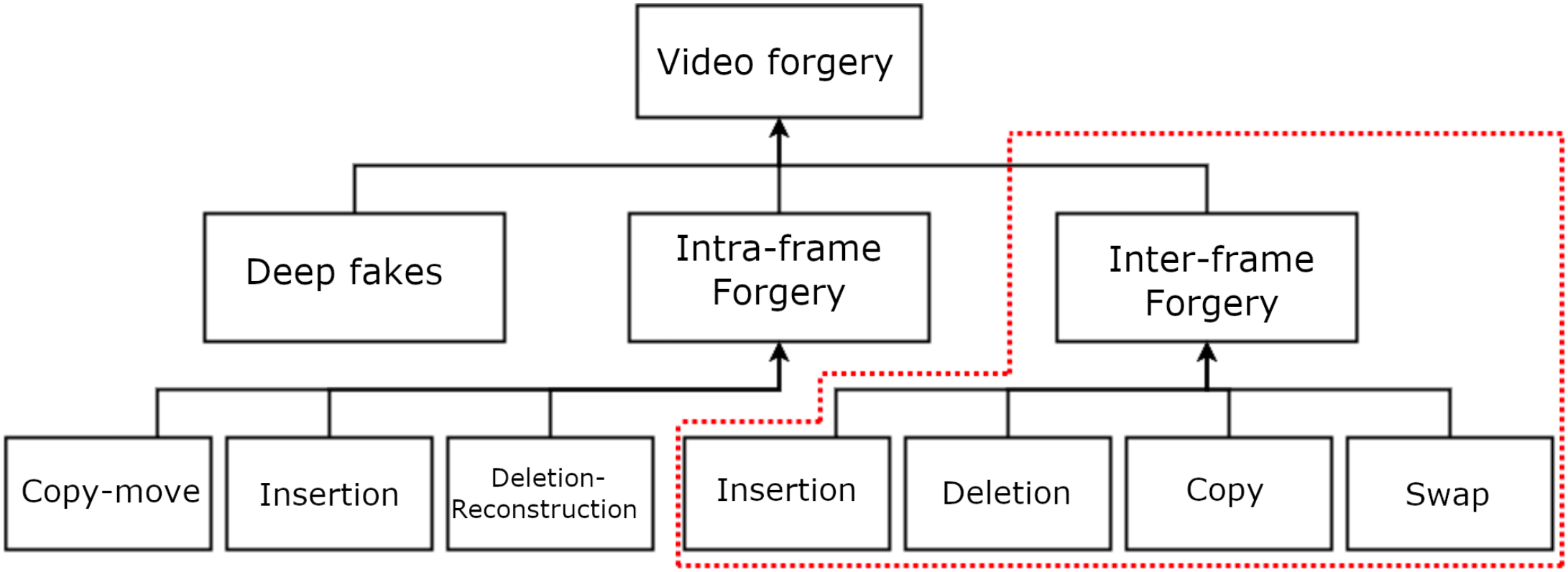
Métrique \ Datasets	Human	Medium Quality Human	Low Quality Human	Complex Human
Human detection	96.6 %	96.3 %	95.6 %	89.1 %

G'DIP FILTERS



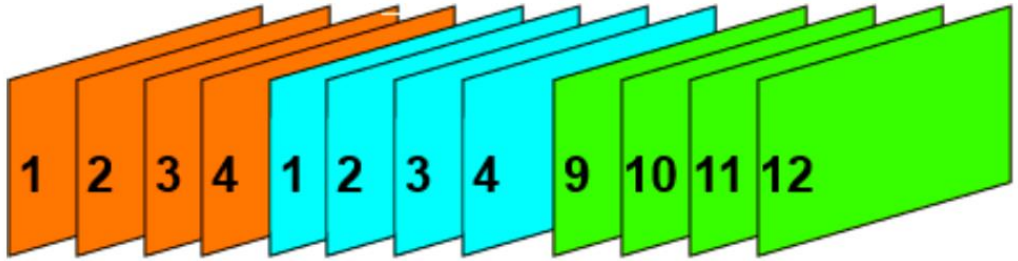
VIDEO – ALTERATION DETECTION

Objective: Has the video been altered?
Hiding pedopornographic content in video

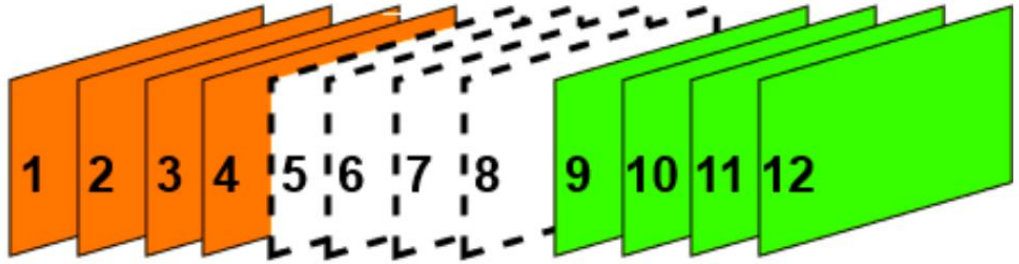


VIDEO – ALTERATION DETECTION

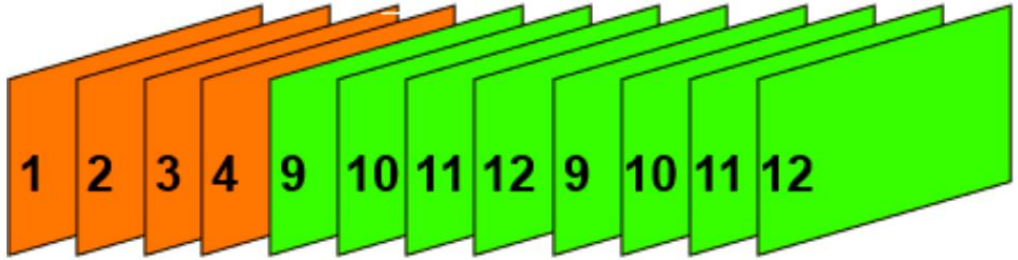
Illustrations:



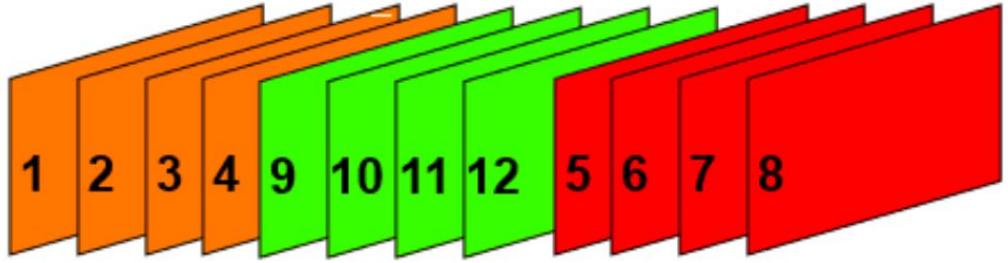
(a) Insertion



(b) **Deletion**



(c) **Copy**



(d) Swap

VIDEO – ALTERATION DETECTION

Principle and performance:

Use of the bitstream for classification

- ❑ No need for the actual video just the encoded file
- ❑ 27 features extracted from the h264 encoded file (bitrate, Quantization parameter QP, QP delta, …), for each one of these we save the mean, min, max and the standard deviation.
- ❑ For each file, we then have a 27 * 4 vector, which can be fed into our classifier

→ **91%** of accuracy

Model	Acc.	AUC	Recall.	Prec˙	F1
L-GBM	**91.63**	**93.55**	97.39	92.6	**94.89**
ADA	91.60	93.4	95.61	**94.16**	94.81
GBC	90.21	93.18	96.96	91.56	94.13
ETC	89.51	89.99	**99.57**	88.87	93.87
RFC	89.16	90.43	98.26	89.44	93.58
LR	87.77	87.85	94.33	91.23	92.51
LDA	87.44	88.49	93.87	91.19	92.3
RC	87.06	0.0	96.5	88.76	92.31
DTC	82.88	71.22	90.43	88.49	89.36
QDA	80.09	75.19	87.39	87.72	87.34
DC	80.09	0.5	1.0	80.09	88.94
KNN	78.04	75.31	89.51	84.14	86.64
SVM	76.56	0.0	89.35	82.81	85.
NB	72.04	84.85	68.99	94.68	79.16

TABLE 1 – Models performance for binary classification

PLAN

- GREYC research lab
- Introduction to digital forensics
- Expert in digital forensics
- G'DIP platform
- Tools illustrations
- **Perspectives**

Normandie Université

GREYC
Laboratoire de recherche en sciences du numérique

PERSPECTIVES

"Nothing is really work unless you would rather be doing something else."

— **J.M. Barrie**

cnrs

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

PERSPECTIVES

Work to do:

- ❑ Finalize platform GUI
- ❑ Adding new tools for disk analysis
  - ✓ Abnormal file location
  - ✓ Filename analysis
  - ✓ Deleted files
  - ✓ …
- ❑ Other digital sources
  - ✓ Internet
  - ✓ Network packets
  - ✓ …

→ Master students projects and internships

→ International collaboration on the subject (with Norway ?)

ON A BESOIN DE VOUS

CREDITS

Project management

- Emmanuel Giguet
- Christophe Rosenberger

Research & development

- Adrien Dubettier

Master students

- Maxime Casati
- Maxime Baud
- Kevin Curtet
- Arthur Fessard
- Bastien Hubert
- Pierre Husson
- Hugo Jean
- Romaric Jollivet
- Antoine Jourdan
- Oscar Mathey
- Benjamin Mauricio
- Leo Metais
- Dorian Napoli
- Alan Patry
- Eva Petauton
- Julien Rauch
- Arthur Rouille
- Nicolas Virard

CONFERENCE

Cyberworlds 2022

September 27(Tue)-29(Thu), 2022

Japan - Kanazawa

Special Track: Cybersecurity

--Cybercrime Prevention:
Identity and trust management, Content protection and digital rights management, Information hiding and anonymity, Privacy protocols, Security protocols, Malware detection, Attack detection, etc.

--Biometrics in Cyberspaces:
Behavioral biometrics, Biometric template protection, Emerging biometrics, Multi-biometrics, Presentation attack detection

--Internet of Things:
Security of embedded systems, Security protocols, Security in V2X and smart cities, Mobile networks security, etc.

--Analysis of Digital traces in Cyberspaces:
Forensics (computer, mobile devices, network, social media), Altered content detection (multimedia, deep fake), Digital data analysis (social media, file carving), etc.

Papers (Full/Short) Submission: ~~April 22, 2022(Fri)~~ **May 27, 2022 (Fri)**
Papers (Full/Short) Notification: ~~May 30, 2022(Mon)~~ **June 27, 2022 (Mon)**

GREYC
Laboratoire de recherche en sciences du numérique

cnrs ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE UNICAEN Normandie Université

QUESTIONS

https://www.greyc.fr/

GREYC

GREYC research lab - UMR CNRS 6072