LES SCIENCES DE L'INVESTIGATION NUMÉRIQUE AU SERVICE DE LA CRIMINALISTIQUE ET DE LA VALORISATION DU PATRIMOINE

Tanguy Gernot, Emmanuel Giguet,
Christophe Charrier, Christophe Rosenberger

Laboratoire GREYC (UMR 6072)
UNICAEN – ENSICAEN - CNRS

G'DIP

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

PLAN

LA PLATEFORME G'DIP

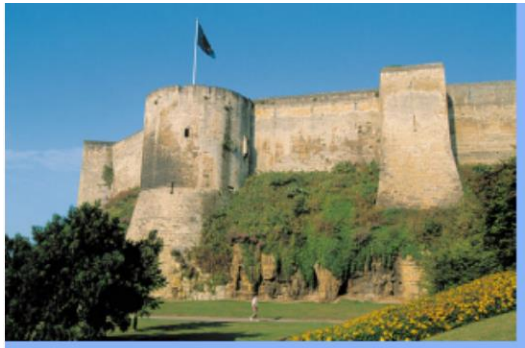
IANEC – INVESTIGATION D'ARCHIVES NUMÉRIQUES

ÉVALUATION COMPARATIVE D'OUTILS D'INVESTIGATION

DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

DÉTECTION DE DEEPFAKE

D'où venons-nous ? (OSINT niveau 0)



LE GREYC
UN LABORATOIRE DE RECHERCHE EN SCIENCES DU NUMÉRIQUE

Traitement d'images, intelligence artificielle, science des données, instrumentation, informatique mathématique, sécurité informatique, traitement automatique des langues ...

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

CARTE D'IDENTITÉ DU GREYC

GREYC CNRS UMR 6072

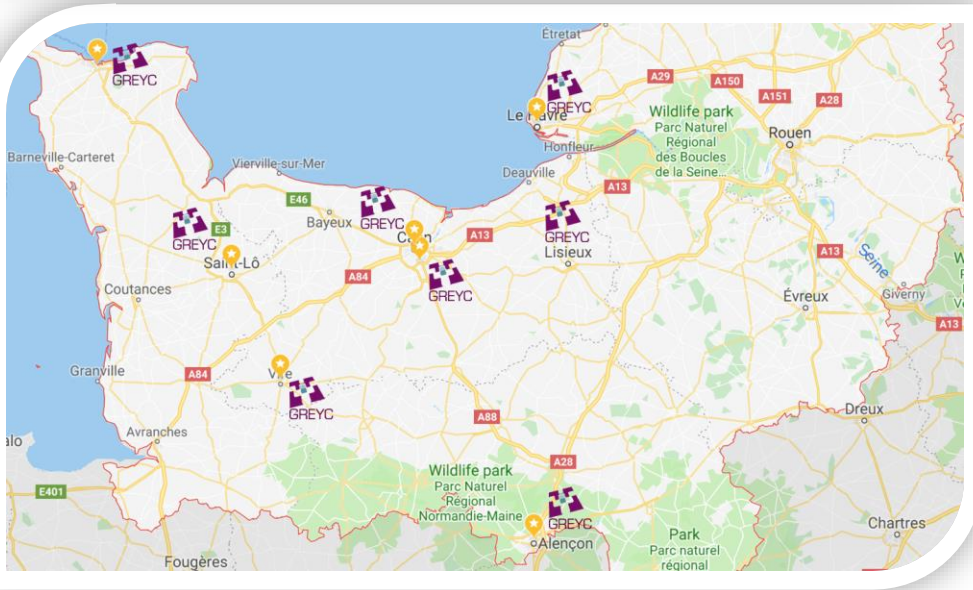
Création : 1995

Effectif : ~180 membres

Budget : 2M€ hors salaires

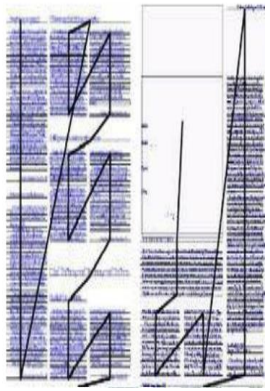
Localisation : 8 sites en Normandie

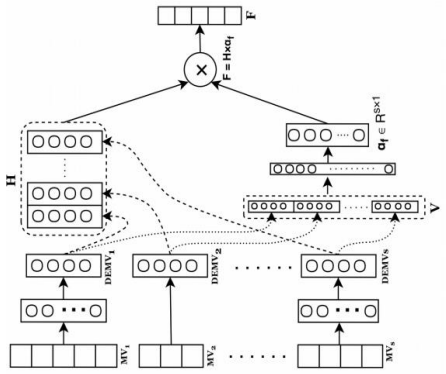
Tutelles : UNICAEN – ENSICAEN - CNRS

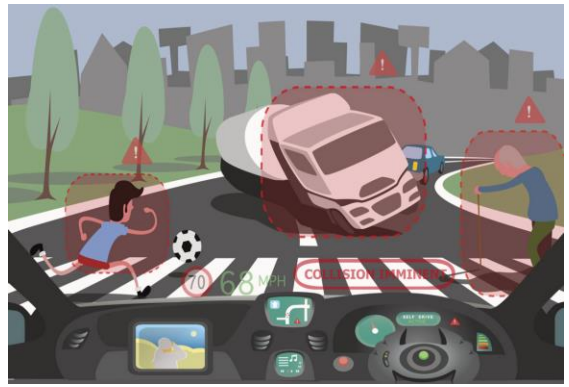


POSITIONNEMENT SCIENTIFIQUE DU GREYC

Recherches fondamentales, méthodologiques et appliquées sur des problématiques relevant des sciences du numérique



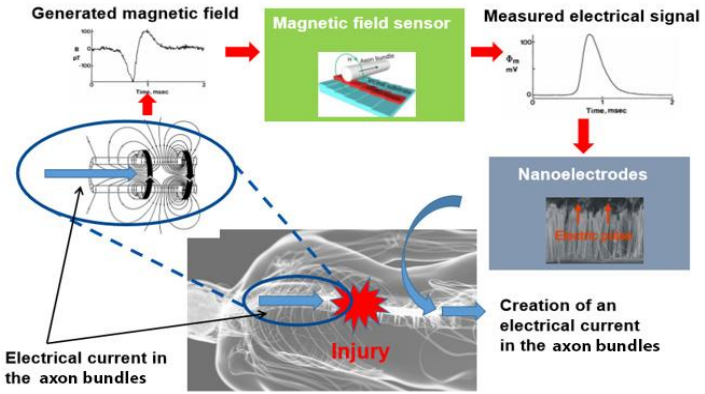


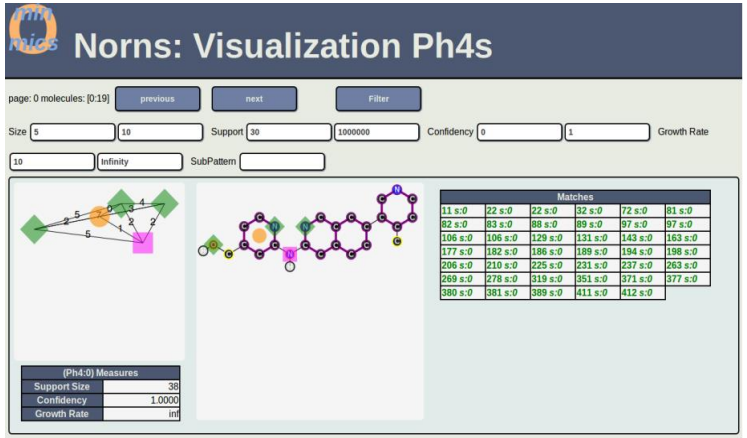


Algorithmes et Intelligence Artificielle

Capteurs et instruments

Science des données





STRUCTURATION SCIENTIFIQUE

6 équipes de recherche:

- **AMACC** : Modèles de calcul, Aléatoire, Combinatoire, Complexité
- **CODAG** : Contraintes Ontologies Données Annotations Graphes
- **MAD** : Modèles, Agents et Décisions
- **IMAGE** : Traitement et interprétation des images
- **ELEC** : Électronique
- **SAFE** : Sécurité, Architectures, Forensique, biomÉtrie

SAFE
UNE ÉQUIPE DE RECHERCHE EN CYBERSÉCURITÉ

Biométrie, sécurité réseau, cryptographie appliquée, protection de la vie privée, analyse forensique…

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

SCIENCE DE L'INVESTIGATION NUMÉRIQUE AU GREYC

Emmanuel Giguet
Chargé de recherche CNRS
Expert judiciaire
près la Cour d'Appel de Caen
de 2005 à 2015

Christophe Charrier
Professeur des Universités
Réserviste Opérationnel
Police Nationale

Tanguy Gernot
Ingénieur de recherche CNRS
Expert judiciaire
près la Cour d'Appel de Caen
depuis 2024

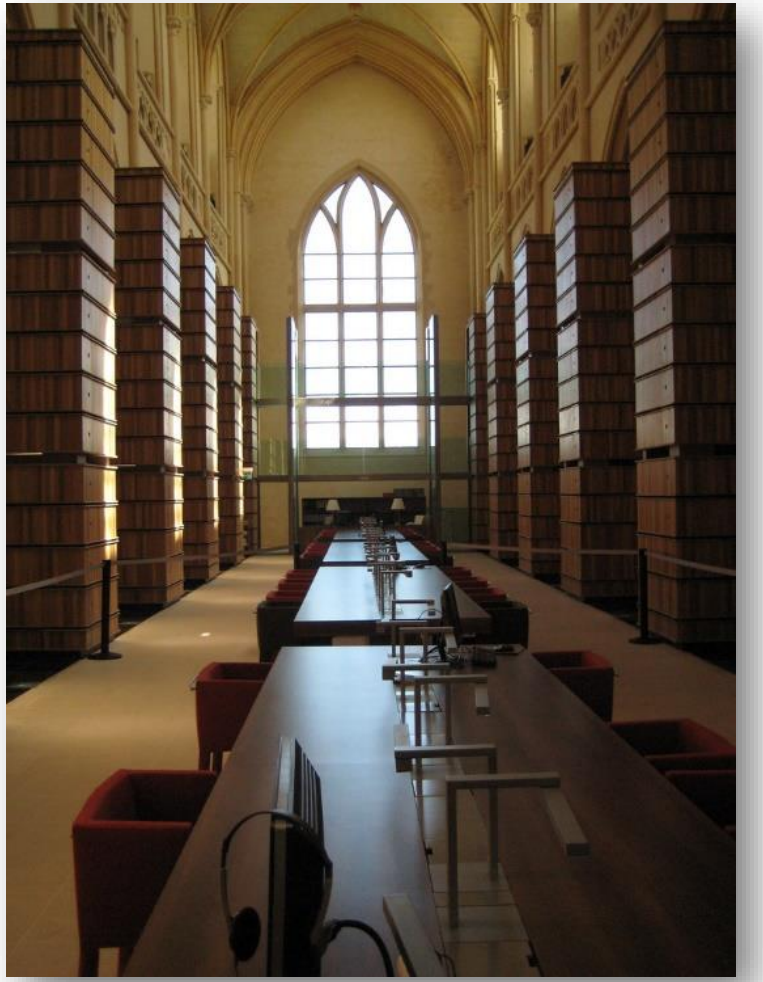
Christophe Rosenberger
Professeur des Universités
Directeur du GREYC

MOTIVATIONS

Axes de travail
- Benchmarking d'outils forensiques
- Création/utilisation de corpus d'évaluation
- Création d’outils, notamment basés sur l’IA
- Publications scientifiques
- Mise à disposition de la plateforme logicielle et d’outils d’analyse

Applications
- Investigation avec la gendarmerie (SR de Caen / C3N)
- Analyse de traces numériques d’auteurs contemporains (IMEC)
- Recherche sur la protection de la vie privée (équipe SAFE)
- Collaborations/contexte applicatif

Conception d’une plateforme logicielle et matérielle
Automatisation de l’analyse de traces numériques de données hétérogènes (disques durs, dumps mémoire, Web, paquets réseau…)



STRATÉGIE PARTENARIALE SUR L'INVESTIGATION

Rectorat Normandie - 2022-2023
Développement G'DIP pour la formation
Module forensique du Master Info
Jeu sérieux prévu 2024

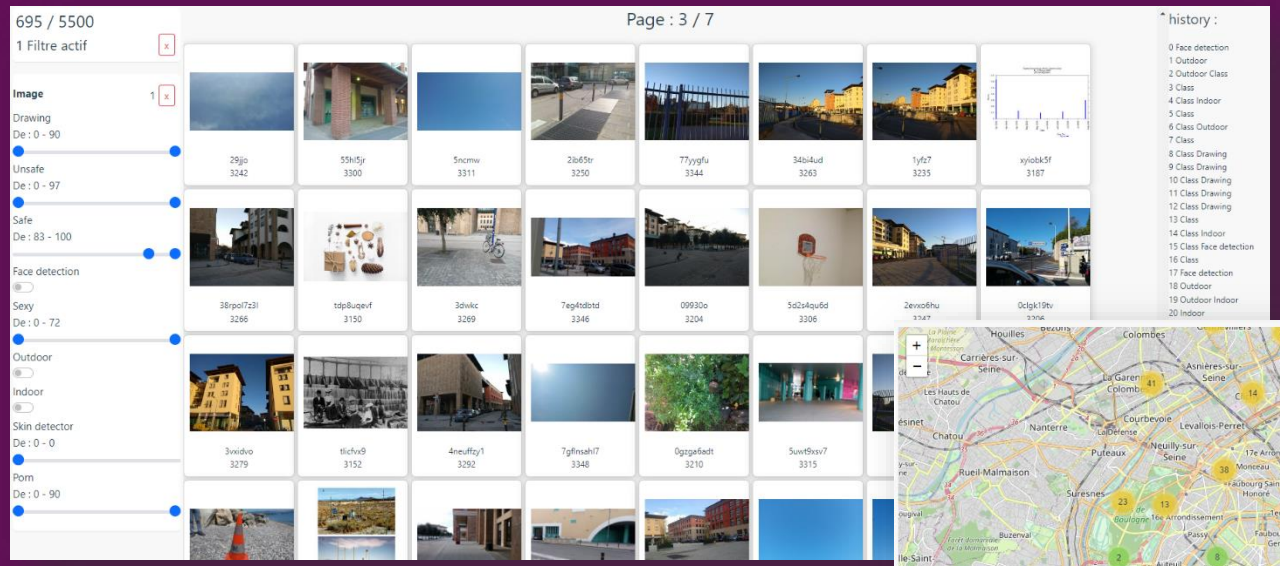
IMEC – 2024-2025
Convention de collaboration
Projet IANEC :
Analyse d'archives numériques

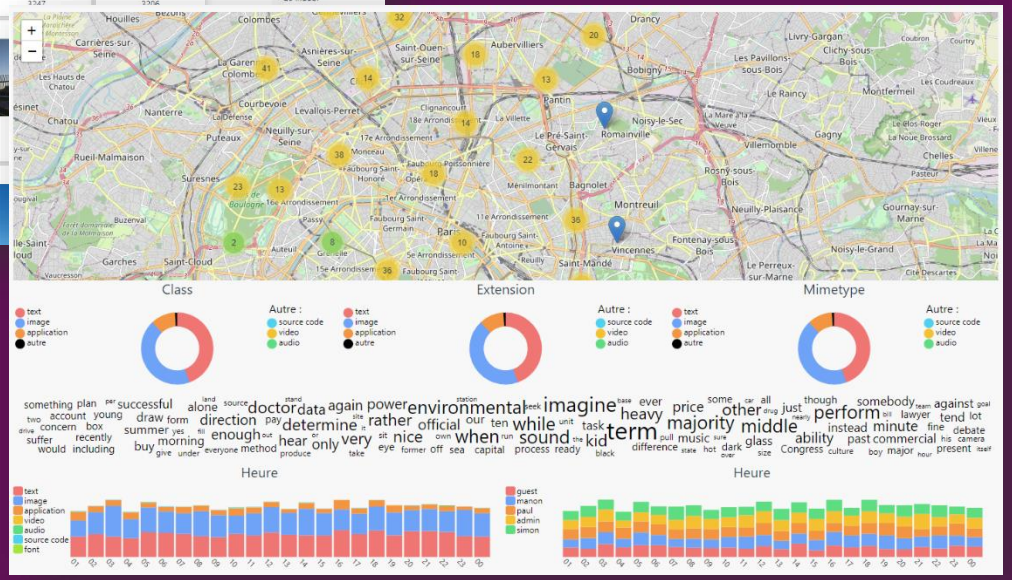
Gendarmerie & Police Nationale
Section recherche de Caen
C3N - COMCyberMI
Recueil du besoin
Avis technique
Conférences

PEPR Cybersécurité
Sécurité multimédia
Thèse sur la détection de deepfakes
Détection des erreurs résiduelles

IRP CNRS AI & CYBER – 2024-2028
Avec la Norvège
(UiO, NTNU, Sintef, Simula, NR)
GT Forensique

LA PLATEFORME G'DIP





G'DIP

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

LA PLATEFORME G'DIP : MOTIVATIONS

Notre Intérêt propre

- Faciliter nos **évaluations comparatives** indépendantes
  - gestion des datasets, filtres « concurrents » intégrés
- Support à nos **partenariats** scientifiques et opérationnels
- Vitrine de notre savoir-faire pour la **médiation scientifique**
- Support à nos **enseignements**
  - Jeu sérieux pour les collégiens et lycéens
  - Formation en master Cyber et module Forensique du master Info

Contraintes & Risques

- Multiplier les plateformes :
  - augmenter le temps de l'analyse (redondance) / les coûts de formation
- Contraintes technologiques :
  - cohérence avec le système d'information des utilisateurs visés / droits des utilisateurs / en local / certification
- Autres choix : faire des modules et des adaptateurs
- Aller vers les choix des partenaires : Go par exemple

G'DIP : CONTRAINTES & SCÉNARIOS

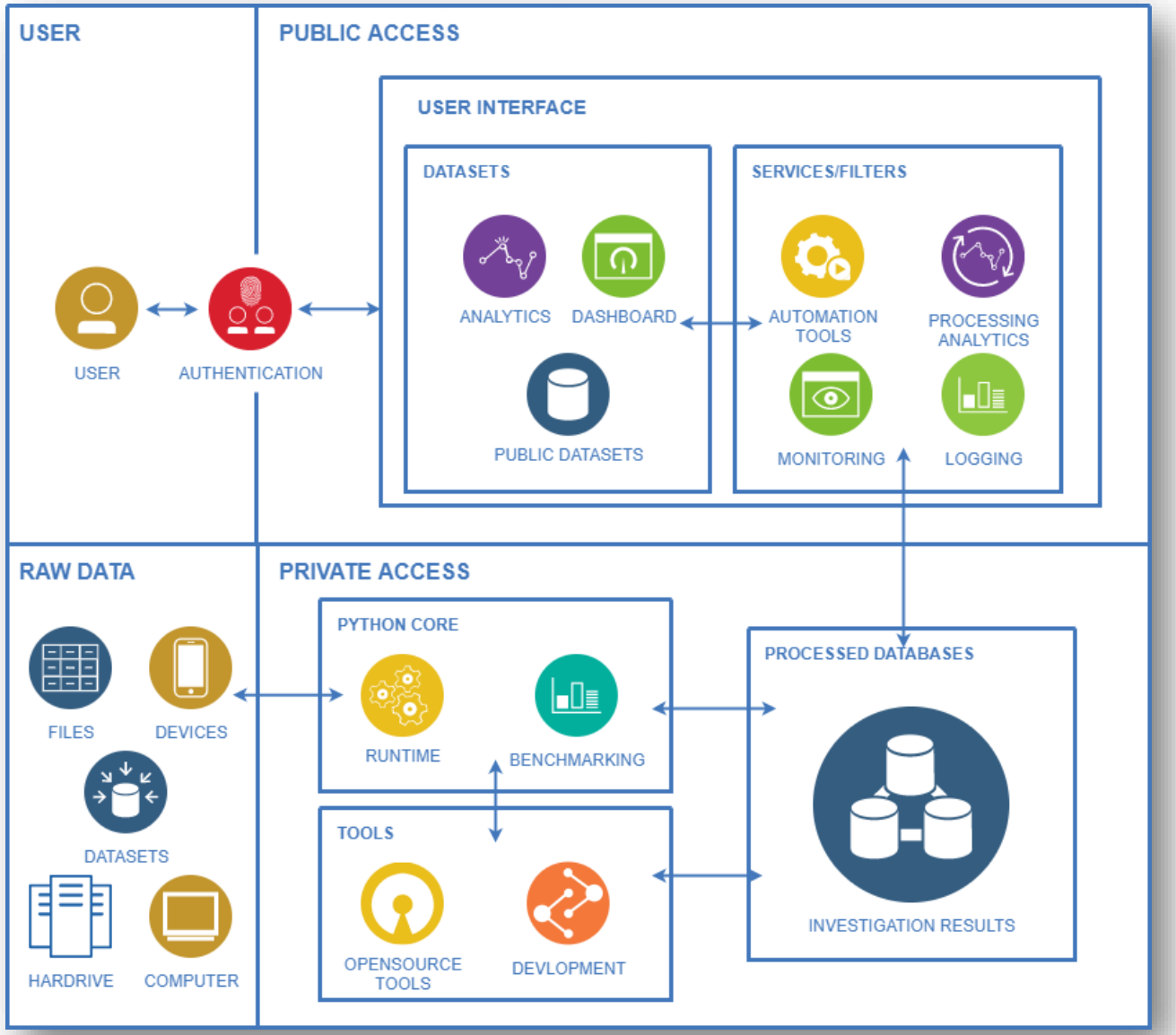
- Trois grands types de mission
  1. Au cours d'une enquête : matériel déjà saisi
  2. En garde à vue
  3. Pendant une perquisition, chez le mis en cause

- Impact du temps sur le scénario d'analyse
  - Reproductibilité et intégrité
    - Analyse directe sur le support
  - Priorisation différente des analyses
    - Traitements longs différés
    - Ciblage des emplacements

- Caractéristiques visées de la plateforme G'DIP
  - Parallélisation des tâches et sous-tâches
  - Priorisation interactive des modules invoqués & Repriorisation dynamique
  - Priorisation interactive des fichiers à traiter :
    - en fonction de la taille / de la date / des emplacements
  - Stratégie d'analyse du déroulé d'un audio ou d'une vidéo :
    - séquentielle, dichotomie, détection de scène
  - Suivi de la progression
    - mise à disposition résultats au fil de l'eau
    - estimation des temps calcul

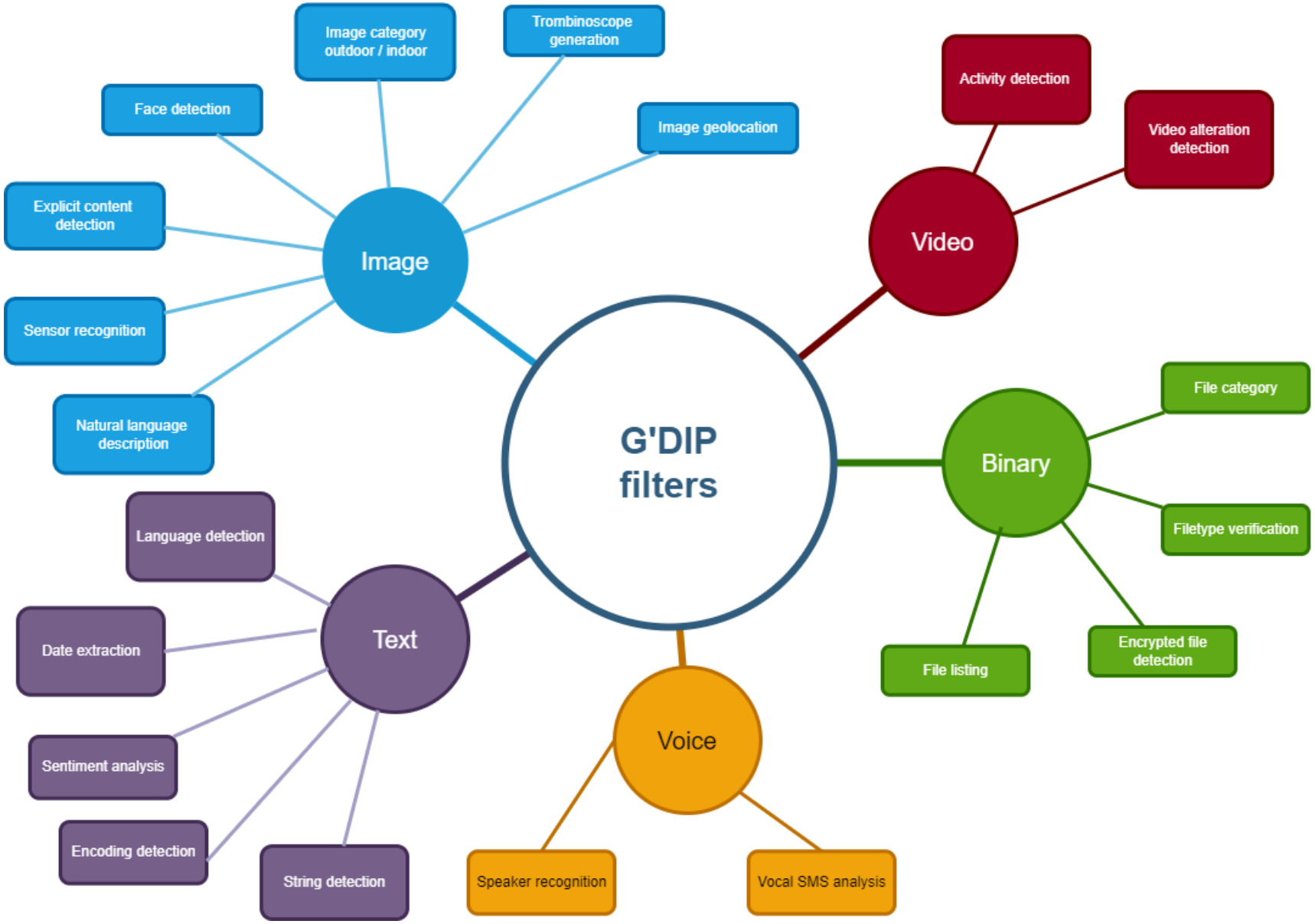
LA PLATEFORME G'DIP

G'DIP



IDDN : FR.001.390004.000.S.P.2024.000.10800

LA PLATEFORME G'DIP



LA PLATEFORME G'DIP : LES FILTRES D'ANALYSE

- Filtres basés sur l'IA
  - Pour le Triage Forensique
  - Aide à la classification
  - Aide à la recherche : cibler des emplacements sur le disque / des périodes

- Modules basés sur l'IA
  - Analyse par le contenu : contenu de photos, de vidéos, de documents,
  - Cohabiter avec les métadonnées
  - « Evite » la question de l'acceptabilité de la preuve
  - Travaux en cours sur intégrant une dimension Explicabilité

- Exemples de filtres
  - Type de fichier
  - Fichier chiffré / non chiffré

  - Scène intérieure / extérieure
  - Géolocalisation par le contenu
  - Présence de visages
  - Caractère explicite sexuel
  - Modèle de capteur photographique
  - Détection de deepfake

  - Détection de tonalité
  - Date
  - Lieu
  - Personnes
  - Organisations

  - Vidéos altérées
  - Vidéos explicites

MOYENS TECHNIQUES À DISPOSITION

Matériel Spécifique de l'équipe

- Bloqueurs / Dupliqueurs
- Tour d'investigation FRED Digital Intelligence
  - GeForce GTX 1050 Ti
  - Intel(R) Core(TM) i7-9800X CPU @ 3.80GHz
  - 64gb RAM
  - 500go ssd

CRIANN : Supercalculateur normand

Cluster AUSTRAL
- 24768 cœurs CPU de calcul
- 88 GPU Nvidia A100 80Go RAM
- 2Po dont 1 en NVME
- 6To RAM

Serveurs de Calcul du Laboratoire

11 serveurs, au total :
- 32 GeForce GTX 1080 Ti 3584 Cores 11Go RAM
- 4 GeForce GTX TITAN X 3072 Cores 12Go RAM
- 8 Nvidia Quadro RTX 6000 24Go RAM
- 26 Intel Xeon E5-2680
- 4352Go RAM
- 80To partagé

JEAN ZAY : Supercalculateur CNRS

89280 cœurs CPU Intel Cascade Lake 6248
214To RAM
1080 GPU Nvidia Tesla V100 SXM2 32 Go
504 GPU Nvidia Tesla V100 SXM2 16 Go
30Po DD
2.5Po SSD

IANEC – INVESTIGATION D'ARCHIVES NUMÉRIQUES

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

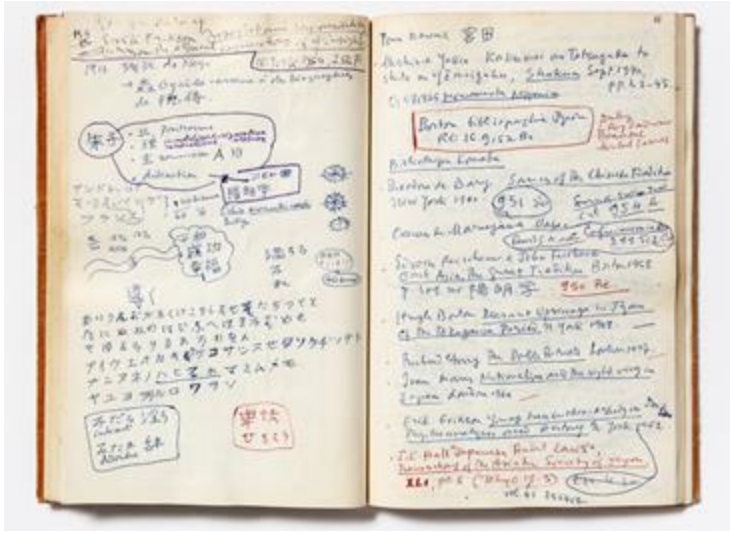
cnrs

L’IMEC : L’Institut Mémoires de l’Édition Contemporaine

L’Institut Mémoires de l’édition contemporaine
Association loi 1901

L’IMEC conserve et met en valeur une importante collection d’archives privées dédiée à l’histoire de la pensée, de l’édition et de la création contemporaine.

Le projet IANEC est financé par le Ministère de la Culture.



Projet IANEC – Les fonds mis à disposition

Fonds fournis au Greyc par l'Imec pour analyse

Fonds 1	Fonds 2	Fonds 3
3 ordinateurs, 373 disquettes, zip iomega, cartouches Syquest	1 Ordinateur	1 Ordinateur, clés USB
Fichiers mac de 1987 à 2004	Fichiers mac de 2000 à 2007	Fichiers mac de 2005 à 2015
Documents texte	Texte, images, documentation	Texte, images, documentation, etc
5 Go - +21 000 fichiers	26,5 Go - 9 812 fichiers	188 Go - 4 images disque

Fonds 4	Fonds 5
1 Ordinateur	1 Ordinateur
Fichiers mac de 2008 à 2019	Fichiers mac de 2005 à 2013
Texte, images, documentation, etc	Texte, images, documentation, etc
21,1 Go - 10 459 fichiers	9,75 Go - 23 946 fichiers

Quelques chiffres :

- 5 fonds / 34 corpus
- ~ 250 Go / 3,5 To totaux

Projet IANEC – Besoins fonctionnels

2 besoins exprimés

Analyse des **caractéristiques techniques** de corpus nativement numériques

Analyse **scientifique** de corpus : identification et description de typologies et de contenu

3 objectifs à atteindre

Caractériser des fichiers numériques natifs, en fonction de typologies de corpus propres aux archives de l'Imec

Collecter des métadonnées descriptives ciblées importantes pour l'identification des documents

Générer une hypothèse de communicabilité des données collectées

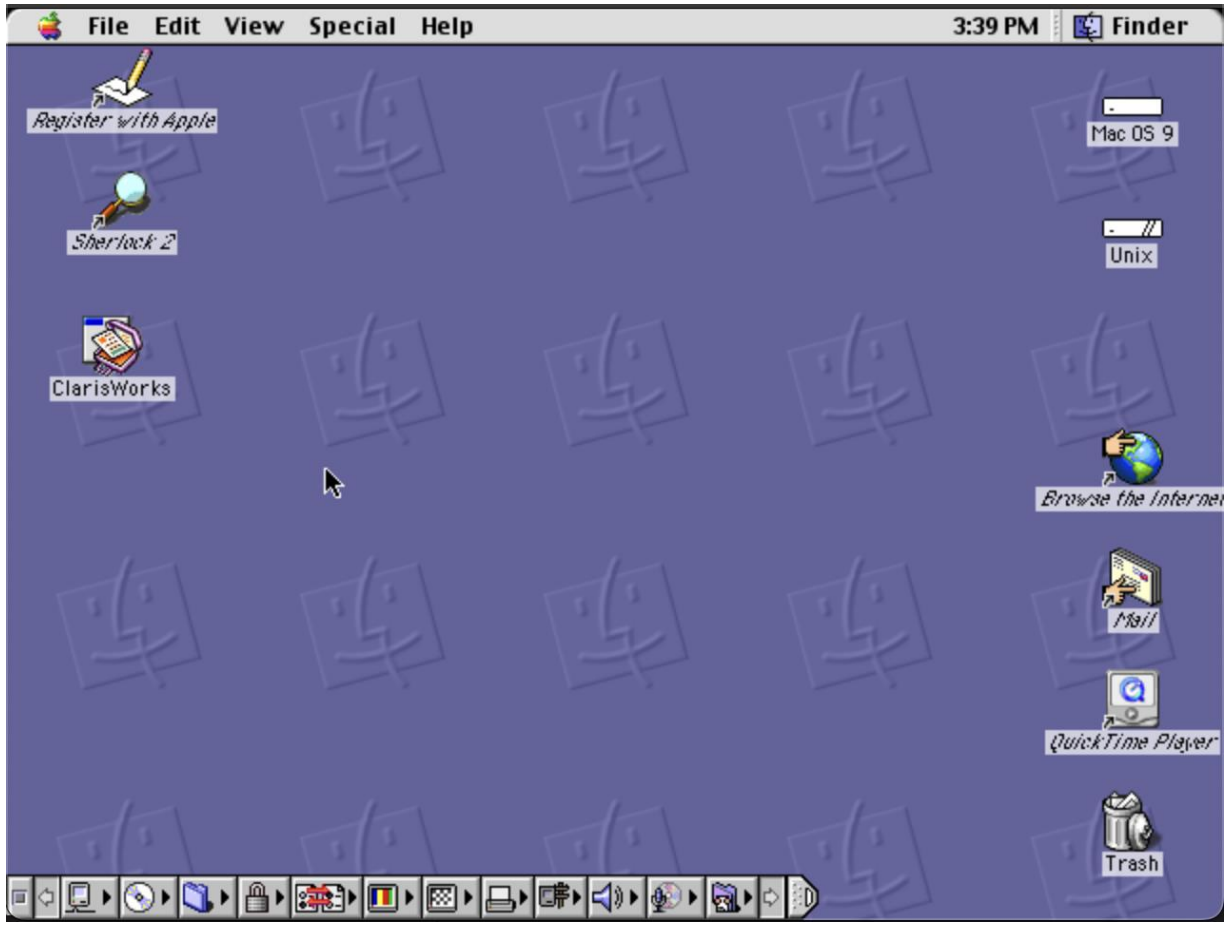
Peut-on redémarrer les ordinateurs pour se retrouver dans la situation de l'auteur ?

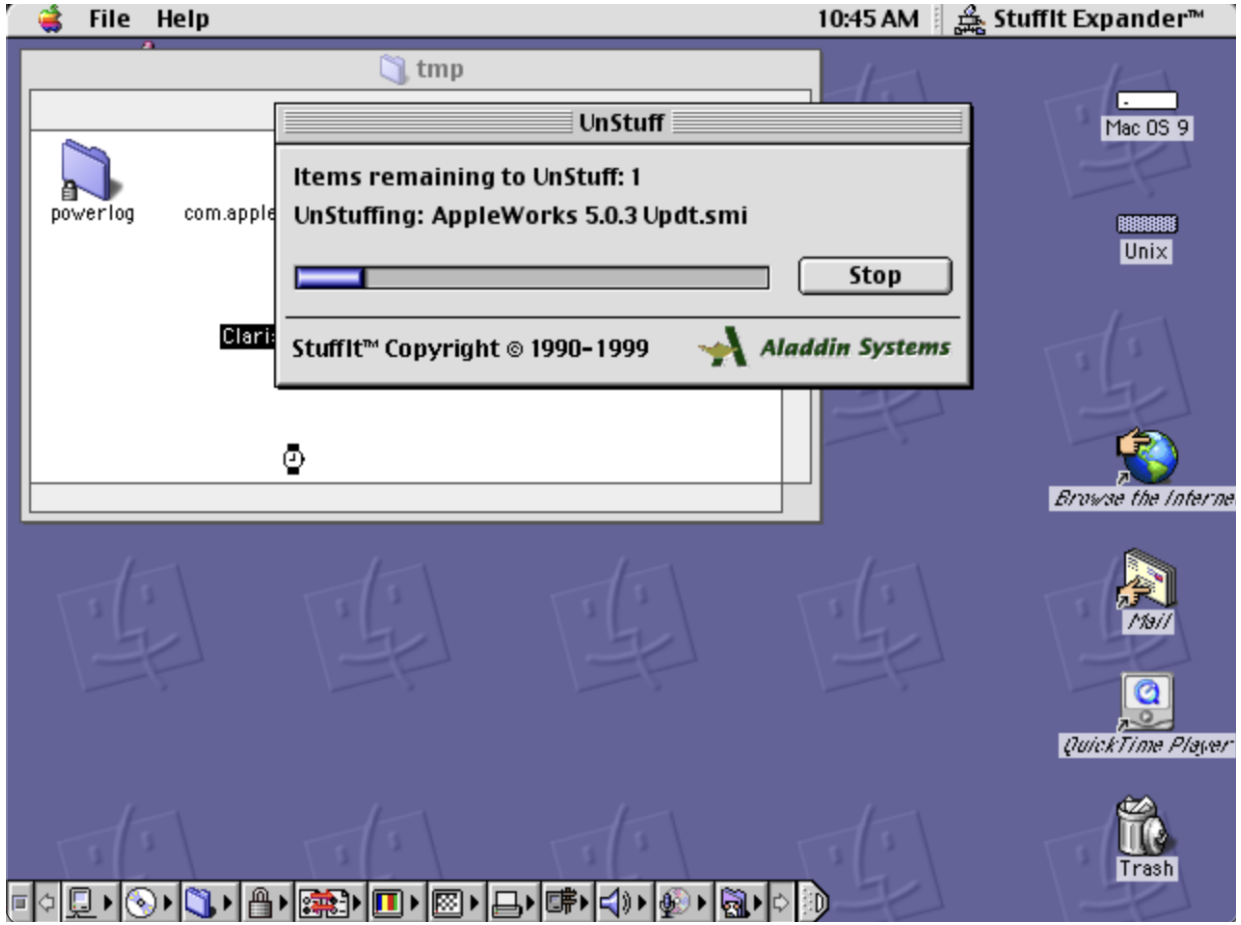
Projet IANEC – Prise en main des données

- Défaut d'intégrité des données sur certaines extractions
  Codage de caractère différents sur la machine hôte

- Modules classiques d'analyse inopérants
  Certains types de fichier ne sont pas ou sont mal détectés
- Accès à certains contenus difficiles
  Format de document plus pris en charge

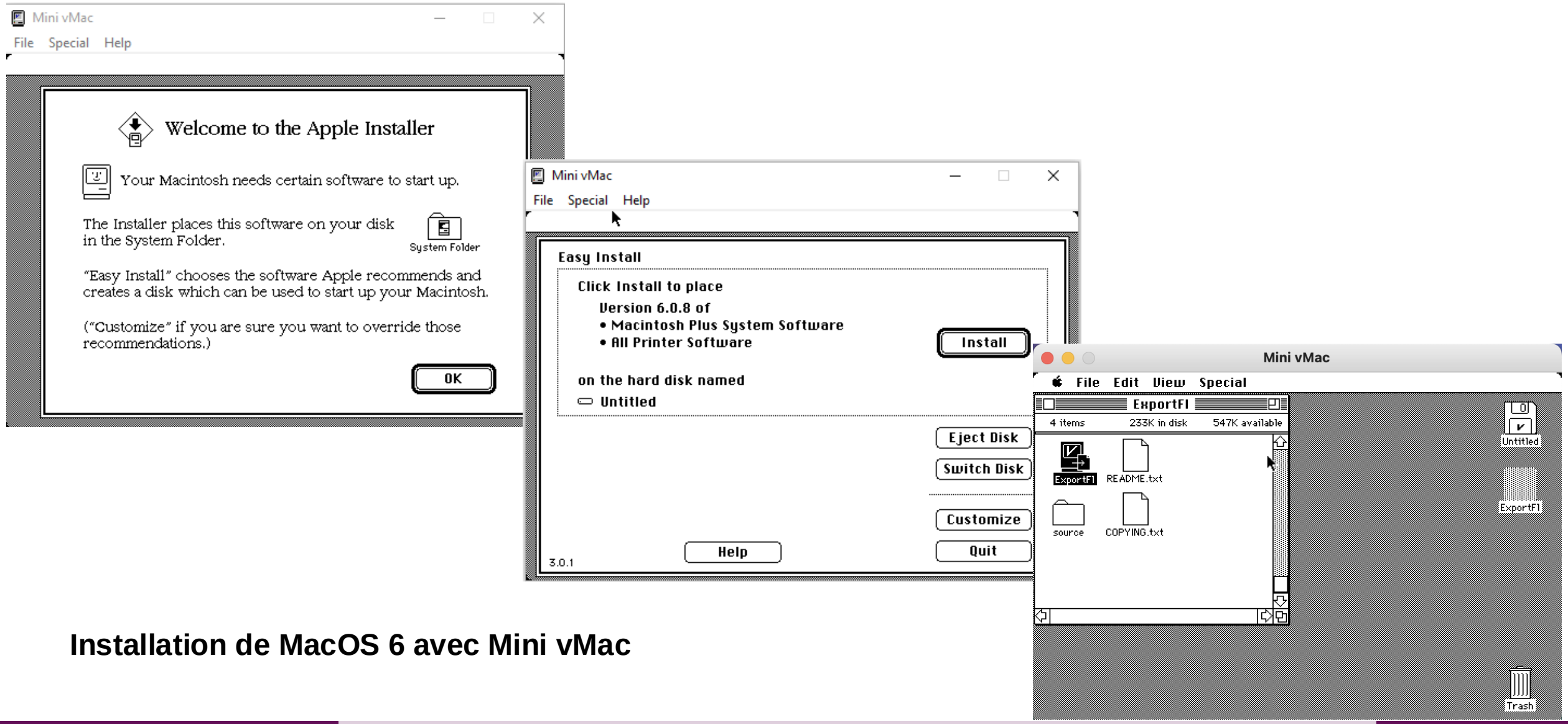
Projet IANEC – Installation des environnements d'origine





Installation de MacOS 7, MacOS 8, MacOS 9, Claris Works, MacWrite, MS Word avec SheepShaver

Projet IANEC – Installation des environnements d'origine



Installation de MacOS 6 avec Mini vMac

Projet IANEC – Intégrité des données

Défaut d'intégrité des noms de fichiers lors du transfert

root/SŽminaire95_6/Hostipita (9)
Zip 100/Bibliographie -? 2003/Bib IIIG-livr. s?JD 2003
Au point2/Par moments, j'ai peur..?
Pour qui... RTF (?)
Bibliographie -? 2003/Bib IIIF-livr. s?JD ???
Žserve rŽcent(double_)/Hopkins 98

"Microsoft's Services For Macintosh feature used U+F001 through U+F029 as replacements for special characters allowed in HFS but forbidden in NTFS, and U+F02A for the Apple logo"

Correctif :

Recodage utf-8 => windows 1252 => macintosh => utf8
UTF-8 => Codepoint => Mapping

http://web.archive.org/web/20180807190401/https://opensource.apple.com/source/ntfs/ntfs-91.50.2/util/ntfs.util.c.auto.html

```
/*
 * Invalid NTFS filename characters are encodeded using the
 * SFM (Services for Macintosh) private use Unicode characters.
 *
 * These should only be used for SMB, MSDOS or NTFS.
 *
 *    Illegal NTFS Char   SFM Unicode Char
 *  ------------------------------------------
 *    0x01-0x1f           0xf001-0xf01f
 *    '"'                 0xf020
 *    '*'                 0xf021
 *    '/'                 0xf022
 *    '<'                 0xf023
 *    '>'                 0xf024
 *    '?'                 0xf025
 *    '\'                 0xf026
 *    '|'                 0xf027
 *    ' '                 0xf028  (Only if last char of the name)
 *    '.'                 0xf029  (Only if last char of the name)
 *  ------------------------------------------
 *
 *  Reference: http://support.microsoft.com/kb/q117258/
 */

/*
 * In the Mac OS 9 days the colon was illegal in a file name. For that reason
 * SFM had no conversion for the colon. There is a conversion for the
 * slash. In Mac OS X the slash is illegal in a file name. So for us the colon
 * is a slash and a slash is a colon. So we can just replace the slash with the
 * colon in our tables and everything will just work.
 *
 * SFM conversion code adapted from xnu/bsd/vfs/vfs_utfconf.c.
 */
static u8 sfm2mac[0x30] = {
        0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, /* 00 - 07 */
        0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f, /* 08 - 0F */
        0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, /* 10 - 17 */
        0x18, 0x19, 0x1a, 0x1b, 0x1c, 0x1d, 0x1e, 0x1f, /* 18 - 1F */
        0x22, 0x2a, 0x3a, 0x3c, 0x3e, 0x3f, 0x5c, 0x7c, /* 20 - 27 */
        0x20, 0x2e                                      /* 28 - 29 */
};
```

Projet IANEC – Intégrité des données

Extrait de résultats :

/Fichiers/syquest2_2018/root/SŽminaire95_6/Hostipita (9)
/Fichiers/syquest2_2018/root/Séminaire95_6/Hostipita (9)

/Fichiers/Zip_100_983A_2017/Zip 100/Bibliographie -? 2003/Bib IIIG-livr. s?JD 2003
/DRR/Fichiers/Zip_100_983A_2017/Zip 100/Bibliographie -> 2003/Bib IIIG-livr. s⁄JD 2003

/Desktop/textes divers/sauvegarde/sauvegarde bureau 3/Mes passions de toujours/versions définitives. Au point2/Par moments, j'ai peur..?
/Desktop/textes divers/sauvegarde/sauvegarde bureau 3/Mes passions de toujours/versions définitives. Au point2/Par moments, j'ai peur...

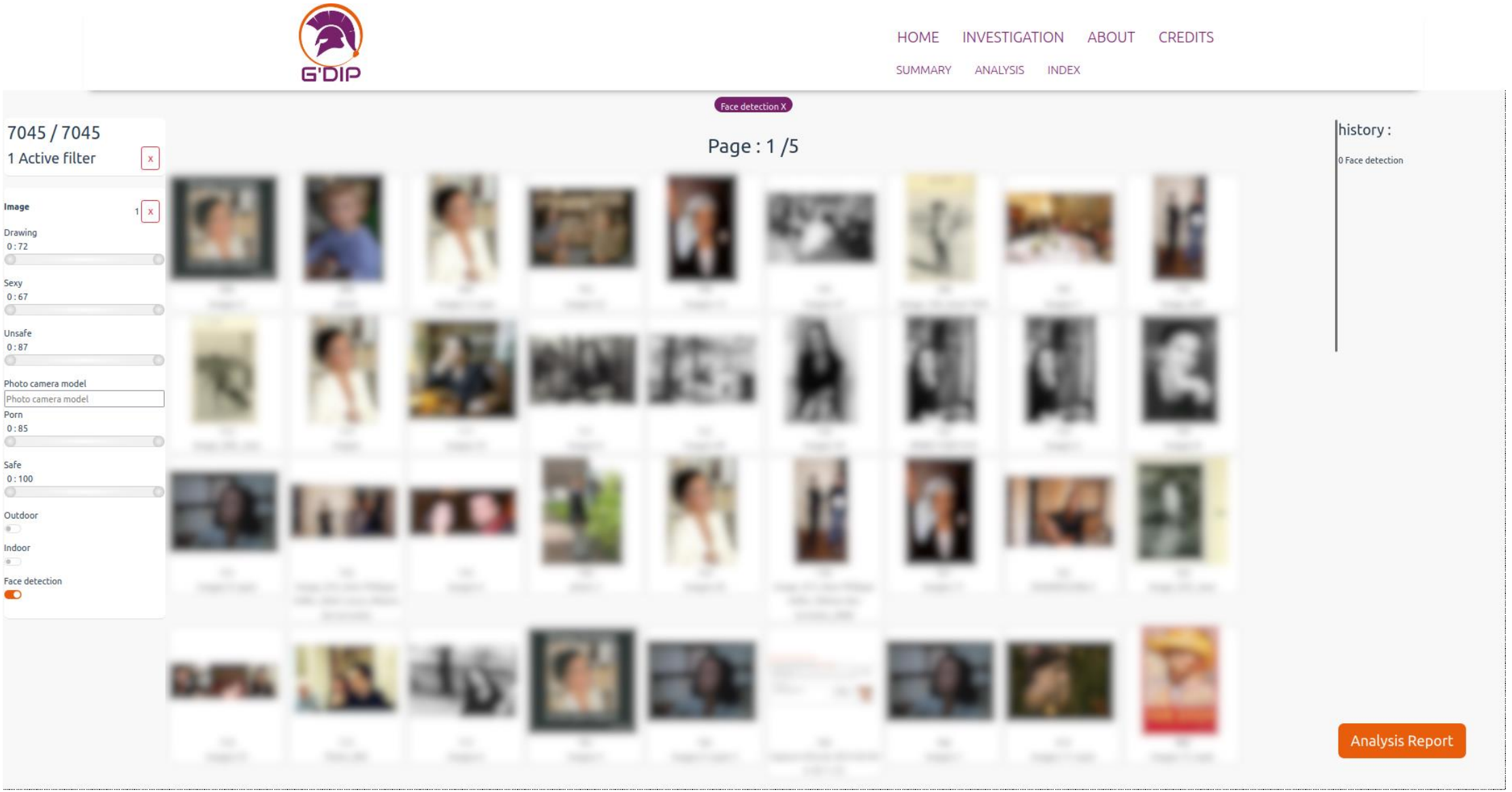
/Fichiers/Zip_100_983A_2017/Zip 100/Pour qui... RTF (?)
/Fichiers/Zip_100_983A_2017/Zip 100/Pour qui... RTF (?)

/Fichiers/syquest2_2018/root/kopi.(Jean)/._Table des mati<U+008F>res
/Fichiers/syquest2_2018/root/kopi.(Jean)/._Table des matières

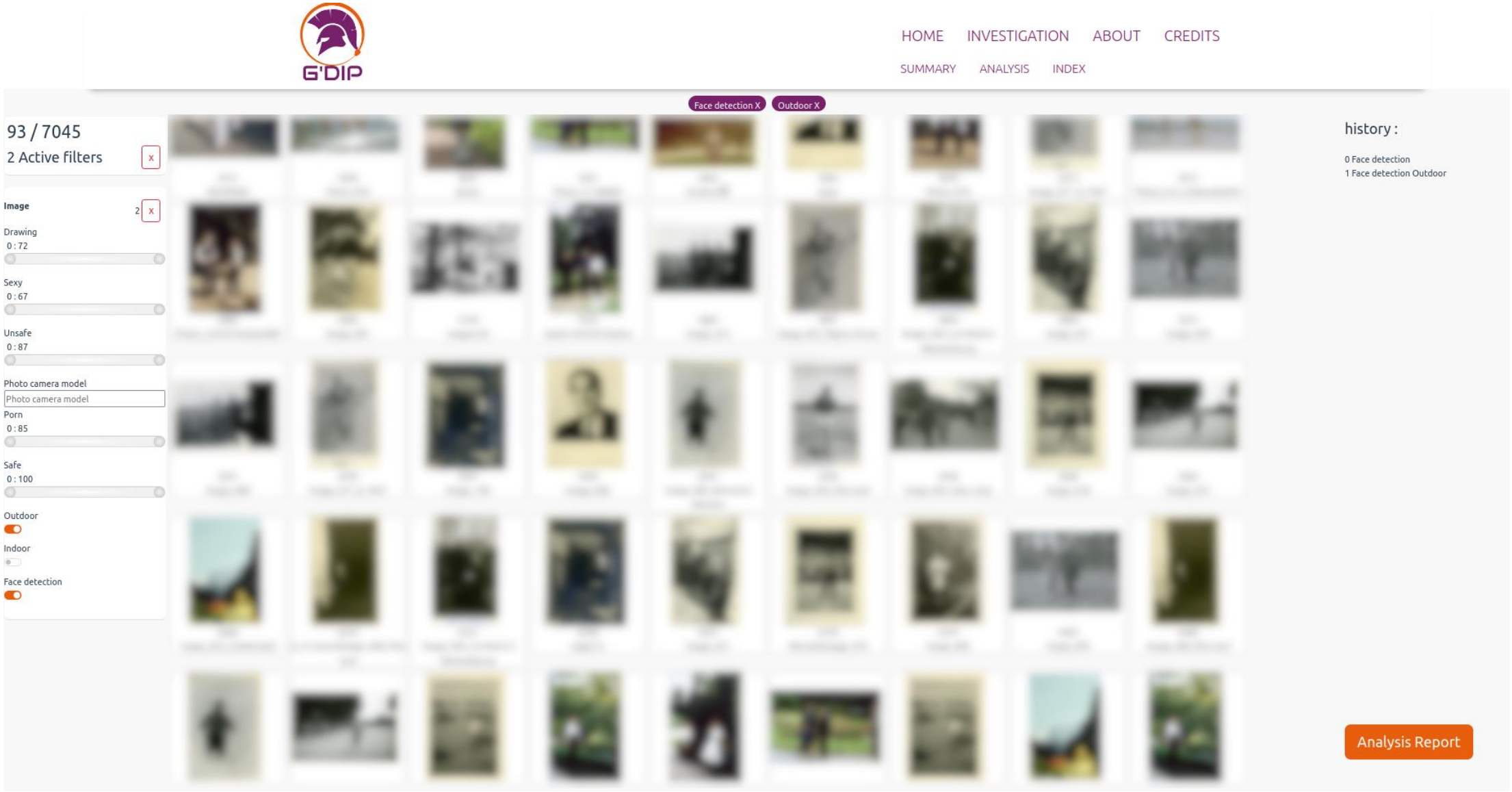
/Fichiers/Zip_100_983A_2017/Zip 100/Bibliographie -? 2003/Bib IIIF-livr. s?JD ???
/Fichiers/Zip_100_983A_2017/Zip 100/Bibliographie -> 2003/Bib IIIF-livr. s⁄JD ???

/Fichiers/syquest1_2018/root/RŽserve rŽcent(double_)/Hopkins 98
/Fichiers/syquest1_2018/root/Réserve récent(double_)/Hopkins 98

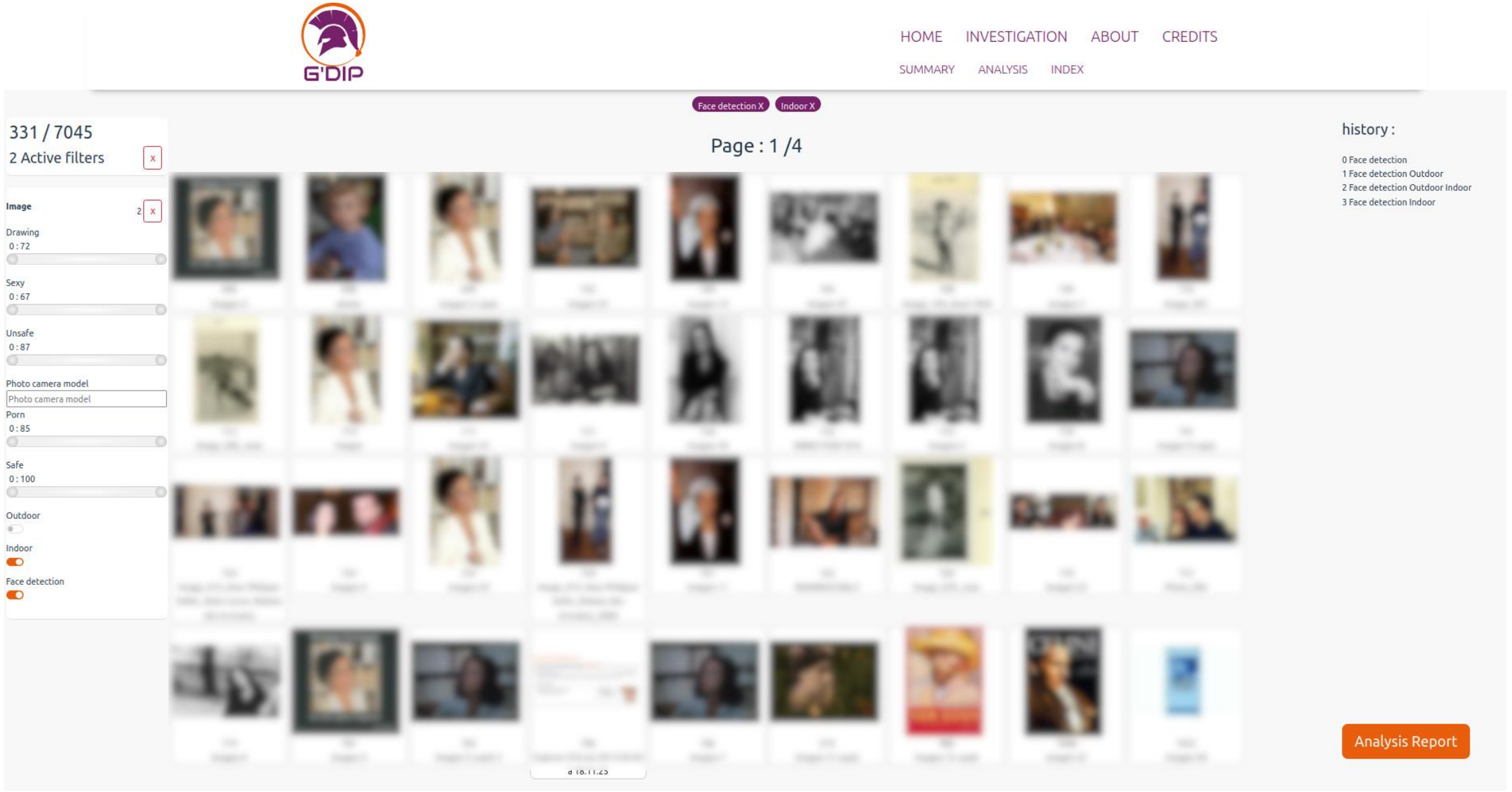
Projet IANEC - Détection de visage



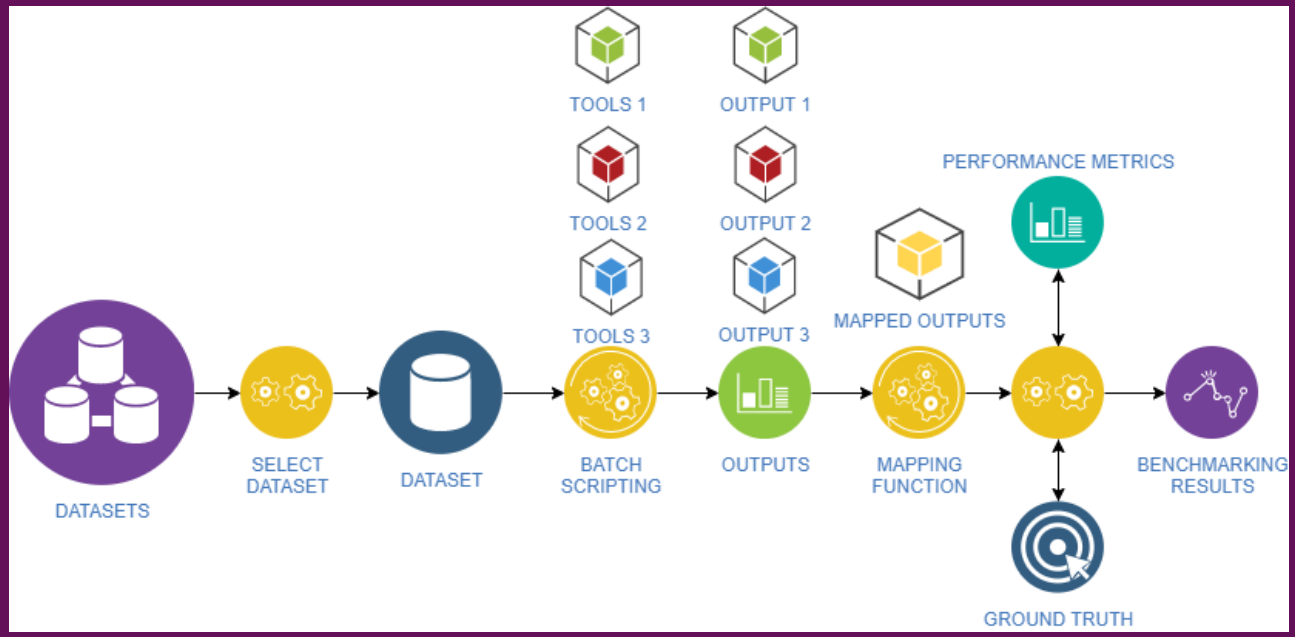
Projet IANEC - Détection de visage en extérieur



Projet IANEC - Détection de visage en intérieur



ÉVALUATION COMPARATIVE D'OUTILS D'INVESTIGATION



GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

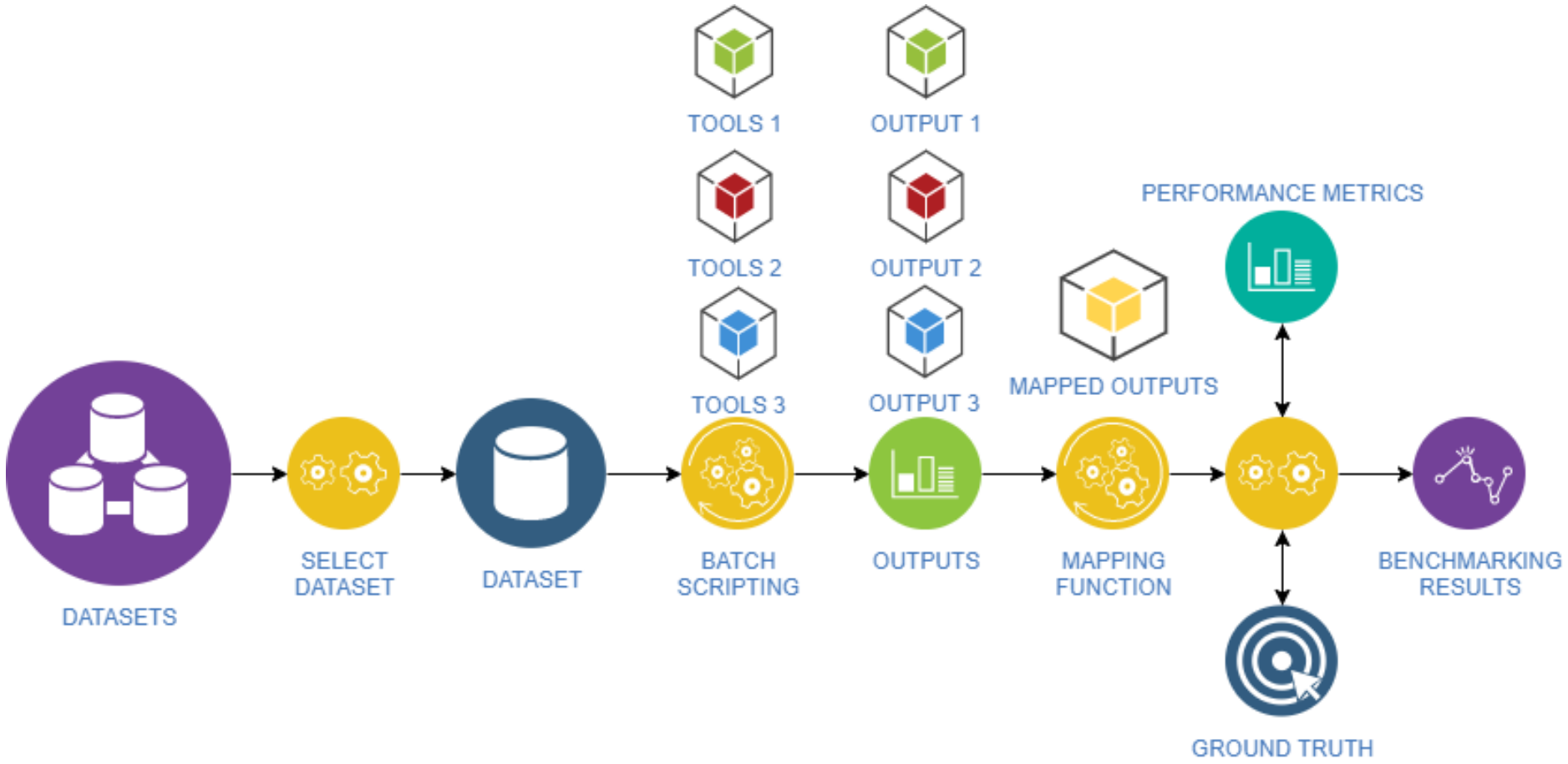
ALTÉRATION DU TYPE DE FICHIER

Objectif : Le type du fichier a-t-il été altéré ?
Méthode pour cacher un fichier sur un PC (exemple: renommer une image porn en exécutable sous windows)
Etat de l'art des solutions de détection

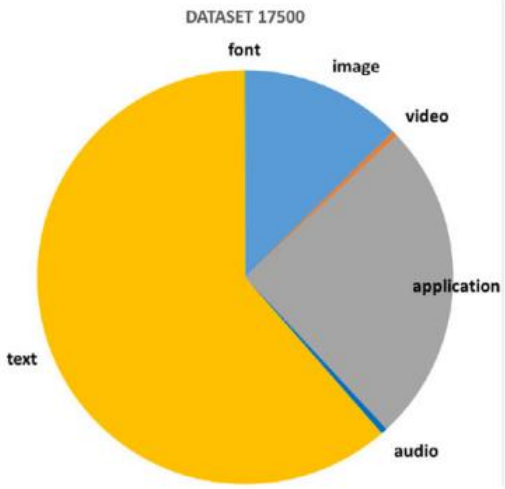
Paper	Year	Principle	#types	Dataset	Accuracy
Sester et al. (Sester et al., 2021)	2021	SVM linear kernel	6	6000	91.4%
Al Neaimi et al. (Al Neaimi et al., 2020)	2020	deep learning	8	4000	99%
Karampidis et al. (Karampidis et al., 2018)	2018	byte frequency distribution + neural network	4	2200	97.6%
Beebe et al. (Beebe et al., 2016)	2016	K-Means, Hierarchical classification	50	2600	74.1%
Evensen (Evensen, 2015)	2015	n-gram analysis with naive Bayes classifier	6	60000	99.5%
Amirani et al. (Amirani et al., 2013)	2013	PCA + Neural Networks feature extraction, SVM	6	1200	99.1%
Cao et al. (Cao et al., 2010)	2010	Gram Frequency Distribution	4	1000	90.3%
Dhanalakshmi & Chellappan (Dhanalakshmi and Chellappan, 2009)	2009	Feature Selection + KNN Classifier	10	5000	90.5%
Software	**Year**	**Principle**	**#types**	**Language**	**Licence**
File (Unix)	1973	magic number + language	338	C	open-source
Fidentify (Grenier, 2019)	2012	magic numbers + binary	440	C	open-source
ForENSIque	2021	magic numbers	155	Rust	open-source
Guess-file-type (Kosinix, 2018)	2018	magic numbers + extension	985	Javascript	open-source
detect-file-type (Paloskin, 2016)	2016	magic numbers	94	Javascript	open-source
filetype (h2non, 2016)	2016	magic numbers	64	Python	open-source
EnCase (Shawn and McCreight, 1998)	2015	magic numbers	406	EnScript/C++	commercial
file-type (Sorhus, 2014)	2014	magic numbers	135	Javascript	open-source
Autopsy (Corp, 2012)	2012	magic numbers + extension	1524	Java	open-source
TrID (Pontello, 2003)	2003	magic numbers	14374	Python	commercial

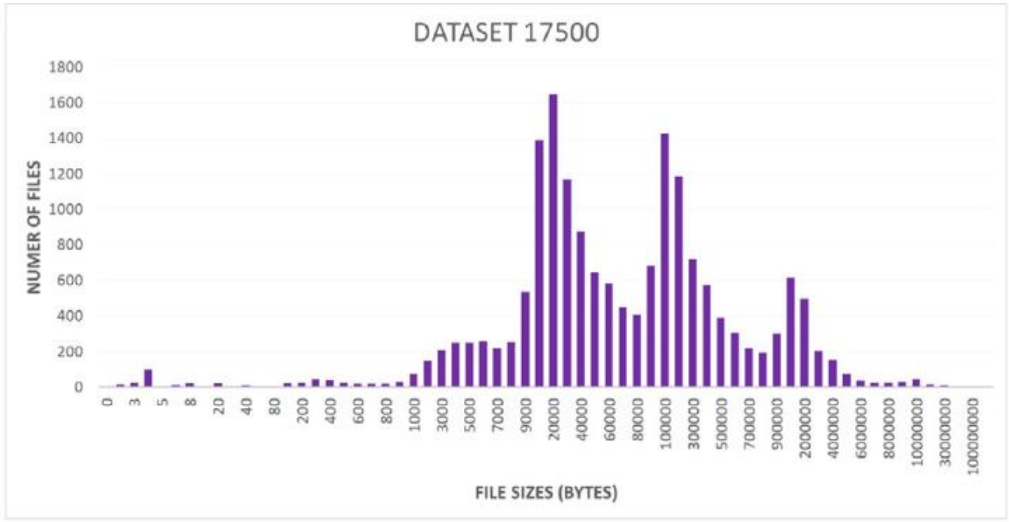
ALTÉRATION DU TYPE DE FICHIER

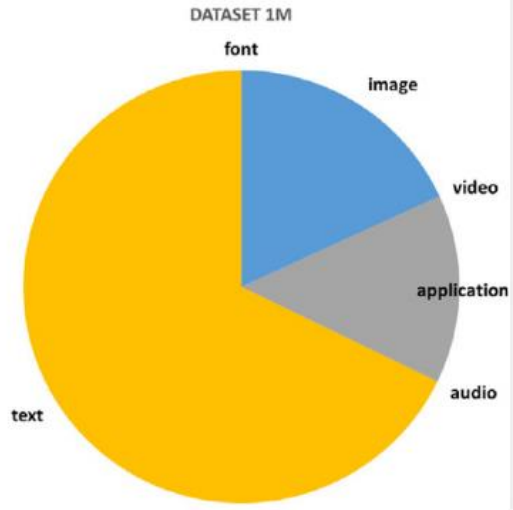
Approche de benchmarking : solutions académiques et commerciales

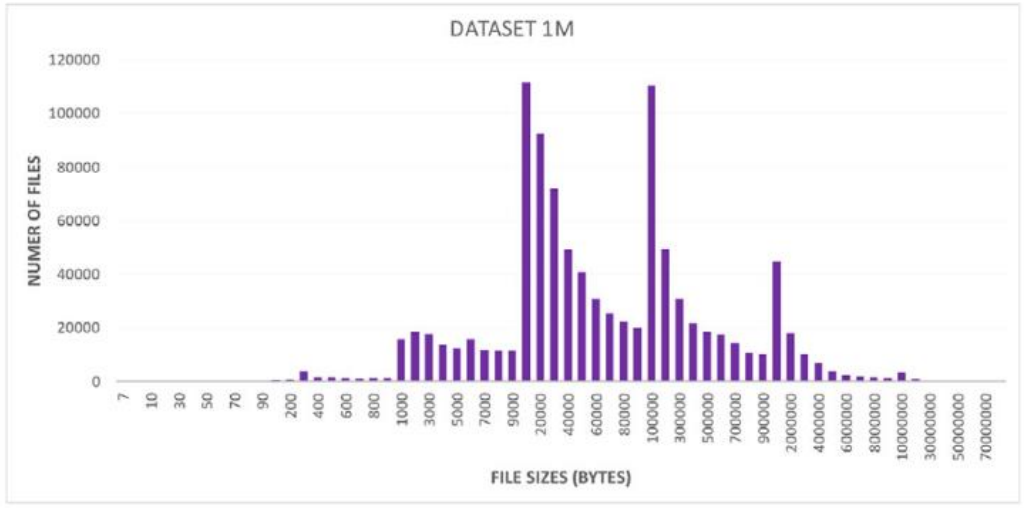


ALTÉRATION DU TYPE DE FICHIER









2 bases de données :

- ❑ 17500, 1M fichiers
- ❑ Différents types de fichier
- ❑ Vérité terrain connue

ALTÉRATION DU TYPE DE FICHIER

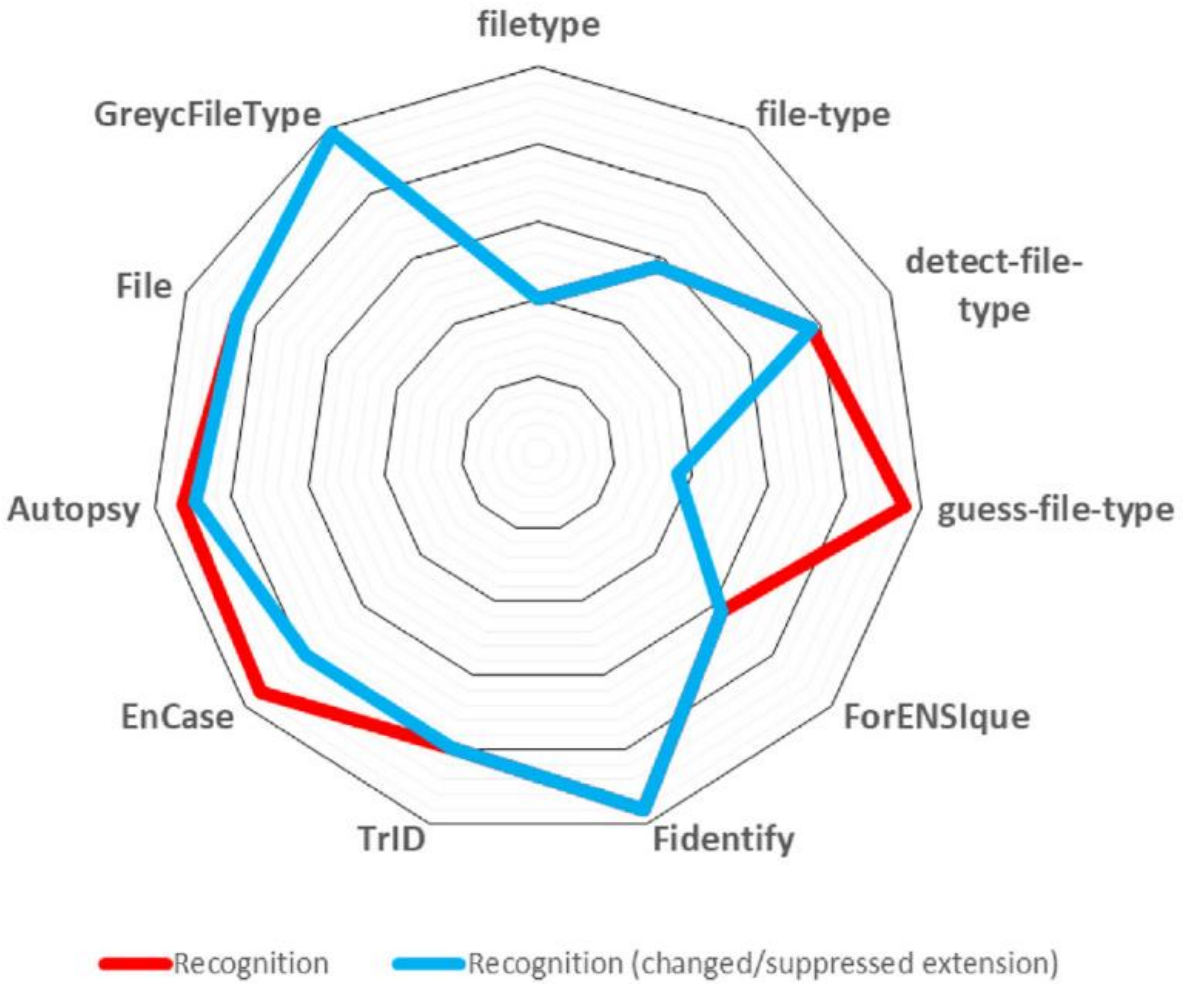
Evaluation de performance :

Accuracy of file type identification for each tested tools on the two datasets.

Tools	17500	1M
filetype	36.2%	43.3%
file-type	49%	65.8%
detect-file-type	74.6%	80%
guess-file-type	34.1%	38.2%
ForENSIque	59.3%	65.8%
Fidentify	**94.4%**	**98.1%**
TrID	74.9%	83.9%
EnCase	77.3%	82.1%
Autopsy	90.6%	88.6%
file	84.7%	85,8%

Meilleure performance de Fidentify (solution open-source)

ALTÉRATION DU TYPE DE FICHIER



Forensic Science International: Digital Investigation 46 (2023) 301574

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

File type identification tools for digital investigations

Adrien Dubettier, Tanguy Gernot, Emmanuel Giguet, Christophe Rosenberger*

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000, Caen, France

ARTICLE INFO

Article history:
Received 23 March 2023
Received in revised form
24 May 2023
Accepted 27 May 2023
Available online xxx

Keywords:
Digital forensics
Digital evidence assessment
Comparative evaluation of forensics tools
Benchmarking
File type identification
File systems

ABSTRACT

Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence for investigation purposes. Building or using file analysis tools is of great interest for a forensic expert to collect high-level information in a short time. In this paper, we consider the examination of files contained in digital media, especially files with possible incorrect types. This often reveals a simple way to hide sensitive content such as porn images, passwords, or accounts. Many commercial and free forensic tools are available for file type identification (FTI). In this work, we assess the performance of ten of them on two significant datasets and scenarios. The main issue we address is the relevance of the tools for forensic purposes. The underlying question is: do expectations meet reality? Our experiments highlight the significant disparity in the accuracy and behavior of the studied tools.

1. Introduction

The scope of Digital Forensics covers the application of forensically sound technologies and methods that deal with the recovery, the investigation, the analysis and the reporting on digital materials and digital traces stored in electronic devices. While Digital Forensics has been raised in the late twentieth century with the increasing prevalence of digital technologies for conducting criminal activities (Caviglione et al., 2017), its scope is now extended to legal activities including Art and Cultural Heritage where digital devices may contain material and traces related to the authors, their work, their creation process, their correspondence (Kirschenbaum et al., Donahue; Dietrich and Adelstein, 2015; Jarlbrink). Whatever the field of application of Digital Forensics, investigative technologies and tools must meet reliability and accuracy requirements (Flandrin et al., 2014). Their performance should be assessed in terms of speed, but also in terms of accuracy, using well-defined formal assessment procedures, in a way to reinforce trust (Bhat et al., 2021; Lazaridis et al., 2016). This is precisely one of the objectives of Digital Forensic Science: contributing to the professionalization of Digital Forensics by providing objective and independent evaluation protocols in order to lead to reproducible results (Horsman, 2019; Casey, 2019; Dimpe and Kogeda, 2019). This aim leads to define evaluation protocols, with explicit guidelines, clear evaluation metrics, and dedicated datasets.

In an operational context, a forensic expert needs to use one or more tools to quickly process files stored in a device. Many commercial off-the-shelf (COTS) products are proposed and many free open-source software are also candidates for this task. It is often difficult to choose the appropriate tools considering performance (computation time), accuracy, cost and usability. These criteria have to be qualified through a rigorous protocol. Furthermore, it is now popular *to blend the models*, that is to combine the output of different solutions to produce a more robust classifier.

In this article, we are interested in the comparative evaluation of file type identification (FTI) tools. After the forensic acquisition process, which includes device write-blocking, device identifier recording and bit-by-bit imaging, determining file types is one of the first investigation processes carried by investigators at an early stage. With the ever-growing need for data storage which leads to increasingly large storage devices, mining the content of disks requires the use of automated tools. In fact, the investigator has to consider devices ranging from one USB stick, to smartphones, laptops, personal computers, hard drives, and terabytes of server disk drives, in order to recover information or to search for evidence (Beckett and Slay, 2007). Automatically determining file types permits to get a quick overview of the storage device content, sorted or filtered by file categories (e.g. office documents, photos, videos, mailboxes), in order to help the investigator (Sindhu and

* Corresponding author.
E-mail address: christophe.rosenberger@ensicaen.fr (C. Rosenberger).

https://doi.org/10.1016/j.fsidi.2023.301574
2666-2817/

Dubettier, A., Gernot, T., Giguet, E., & Rosenberger, C. (2023). File type identification tools for digital investigations. *Forensic Science International: Digital Investigation*, *46*, 301574.

DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

GREYC
Laboratoire de recherche en sciences du numérique
Normandie Université
UNICAEN
ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE
cnrs

DÉTECTION DU CARACTERE EXPLICITE SEXUEL

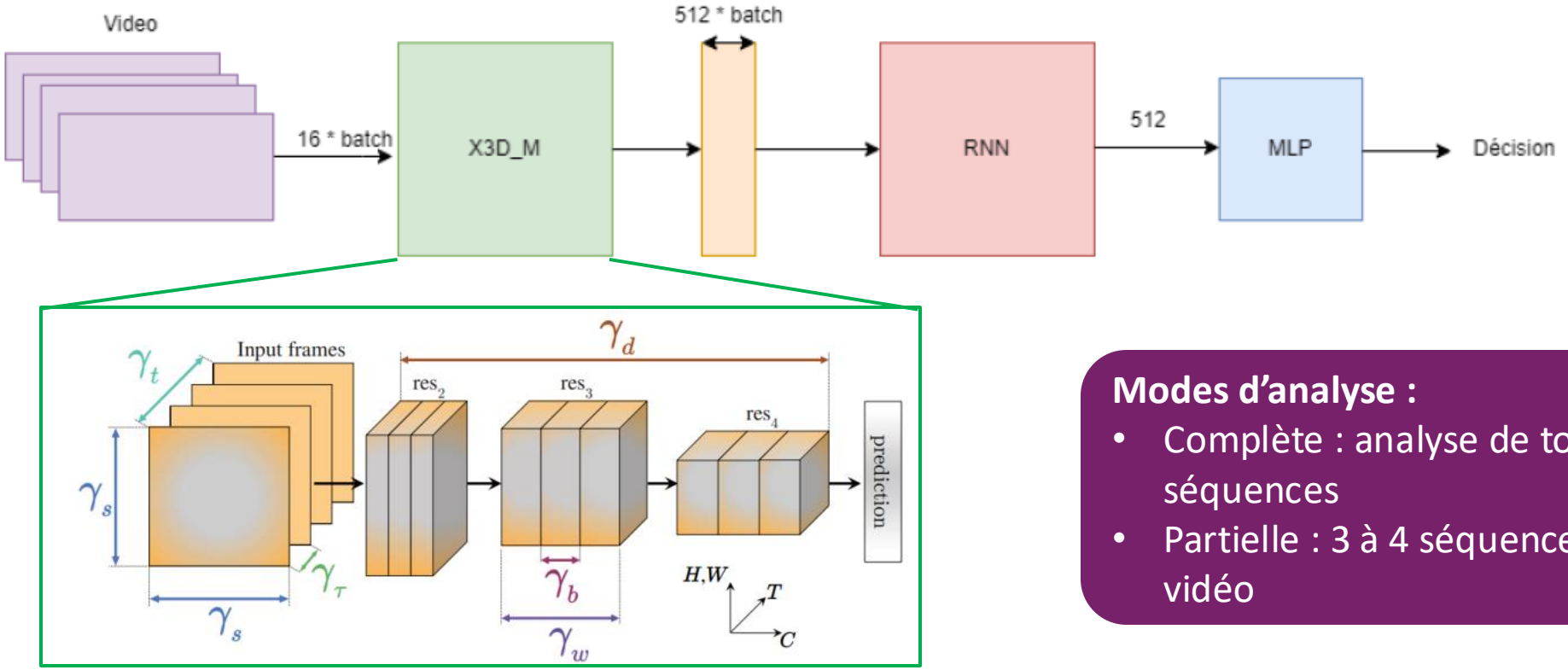
Objectifs :
Proposer une méthode performante (rapide et efficace) d'analyse de vidéos pour détecter du contenu explicite à caractère sexuel

Applications :
- Faciliter des investigations numériques dans des enquêtes criminelles pédopornographiques
- Possible filtre de protection pour des enfants
- Vérification automatique d'upload de vidéos

DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

Méthode proposée :

- Réseau de neurones convolutionnels pour la génération de descripteurs de clips vidéo (taille 512 x 16 frames)
- Réduction de la taille du vecteur par un réseau de neurones récurrent sur le caractère explicite (taille 512)
- Prédiction par un perceptron multi-couches
- Apprentissage avec un jeu de données de 4000 vidéos



Modes d'analyse :

- Complète : analyse de toutes les séquences
- Partielle : 3 à 4 séquences de la vidéo

DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

Contributions
Proposition de modèles efficaces (audio, vidéo, audio + vidéo), 85ms pour la prédiction

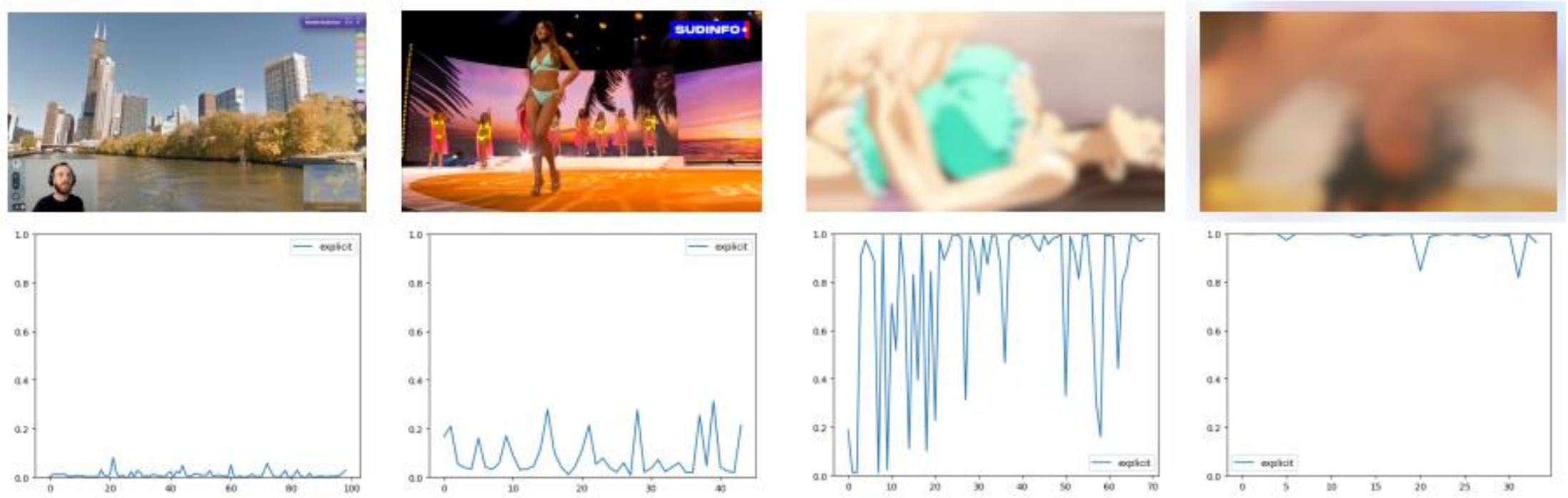
Multimedia content	References	Accuracy	Size(Mb)	Dataset
Audio	**Contribution (audio model)**	85.6%	**7.3**	LSPD (audio)
Image	Open NSFW + SVM [20]	85.76%	22.7	NPDI-2k
	ShallowCNN(AlexNet) [20]	84.56 %	-	NPDI-2k
	Open NSFW + MaskR-CNN [21] [22]	90.4%	182.4	NPDI-2k
Video	YOLOv4 [23]	87.75%	246	LSPD
	SSD[24]	83.28%	100	LSPD
	Cascade Mask R-CNN [19]	86.63%	319	LSPD
	Contribution (video model)	**96.0%**	16	LSPD
Audio + Video	**Contribution**	93.3%	23.3	LSPD (audio)

Comparison of contributions in the field of sexual explicit content detection in multimedia content.

Jean, H., Giguet, E., & Rosenberger, C. (2023, June). Détection de contenu explicite dans les vidéos. In *Conférence CORESA (COmpression et REprésentation des Signaux Audiovisuels)*.

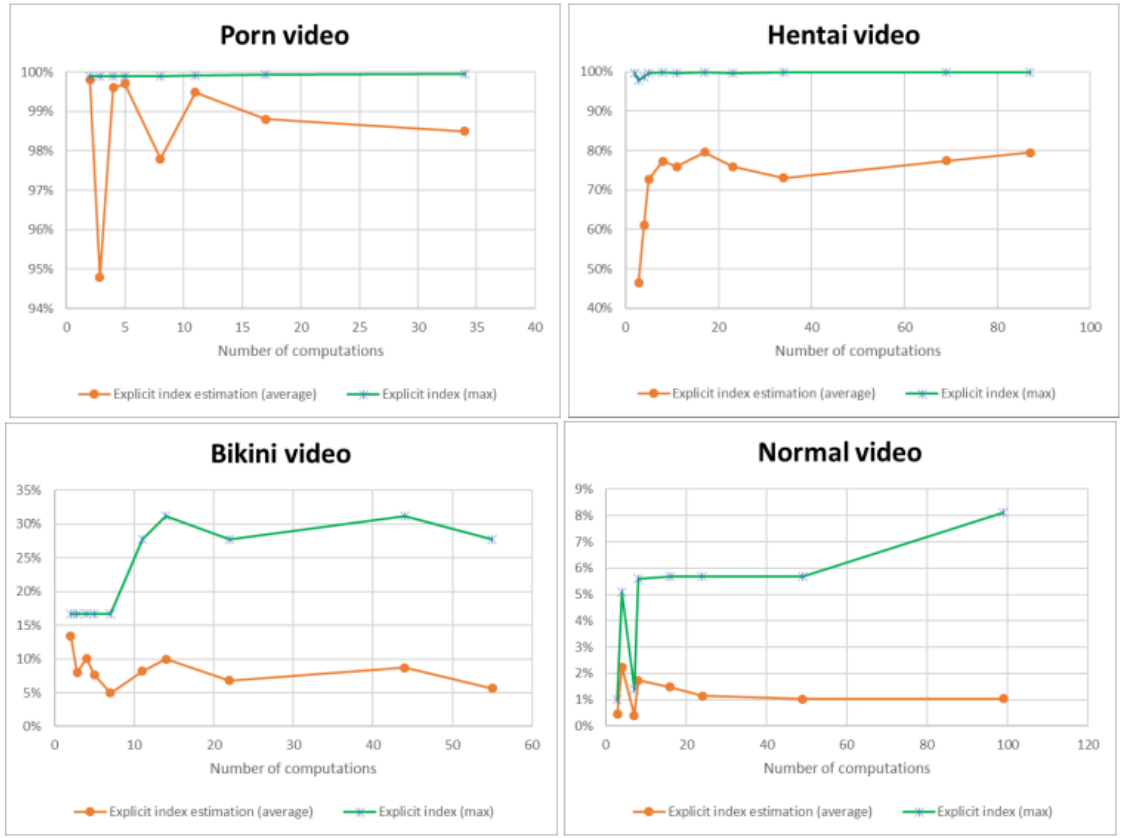
DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

Illustration
Analyse de différentes vidéos (normal, bikini, hentai, porno)



DÉTECTION DU CARACTÈRE EXPLICITE SEXUEL

Illustration
Analyse de différentes vidéos (normal, bikini, hentai, porno)



DÉTECTION DE DEEPFAKE

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

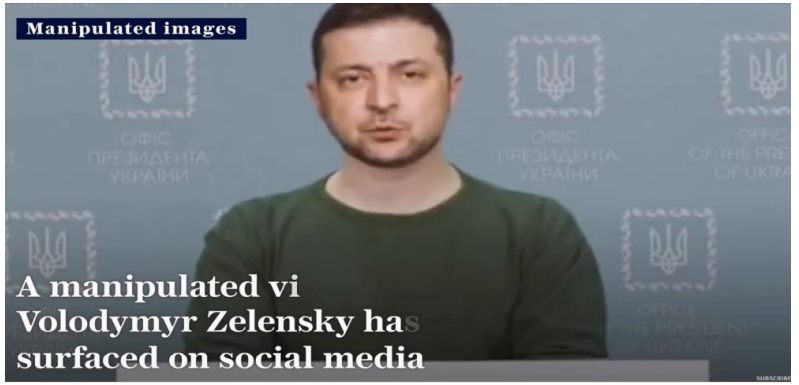
DÉTECTION DE DEEPFAKE

Objectifs :

- Proposer une méthode de détection de deepake alliant explicabilité et réseaux légers
- Cibler les échanges de visage

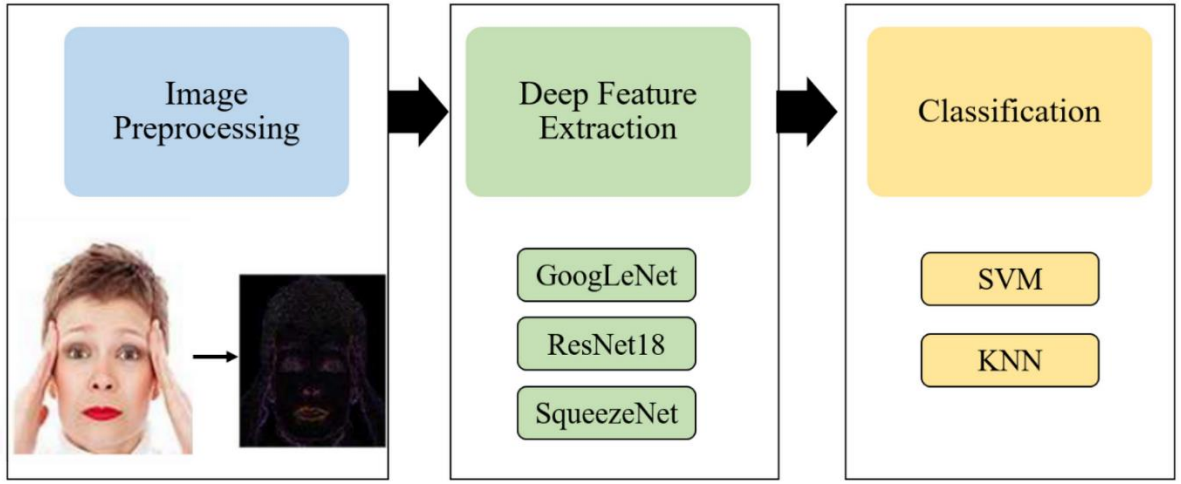
Applications :

- Lutter contre la désinformation (fake news)
- Lutter contre le cyberharcèlement (revenge porn, etc)



Détection de Deepfake : analyse de l'état de l'art

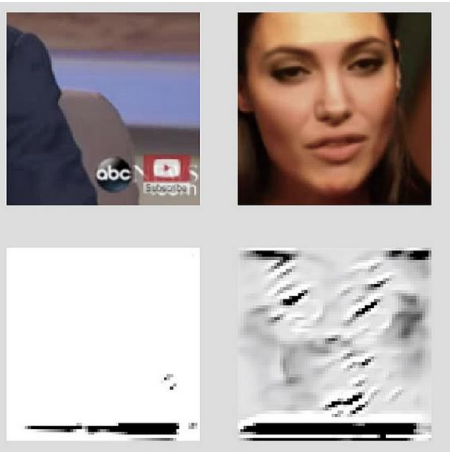
- Nombreuses méthodes proposées pour détecter les vidéos falsifiées.
  - Détection basée sur un réseau neuronal convolutif général (CNN)
  - La détection de fausses vidéos est généralement considérée comme une tâche de classification.



- Bonne performance de généralisation, mais
  - Seulement des informations globales à partir des indices extraits
  - Utilisation de modèles d'apprentissage complexes
  - Augmentent la complexité des calculs et la difficulté de l'apprentissage

Détection de Deepfake : l'approche proposée

1. Considérer les signaux résiduels
   - Invisibles à l'œil et ressemblant à une signature cachée
2. Comment les signaux résiduels peuvent-ils être analysés image par image dans le domaine spatial et fréquentiel ?
3. Les caractéristiques basées sur les signaux résiduels peuvent préserver les traces de manipulation et supprimer le contenu non pertinent de l'image.

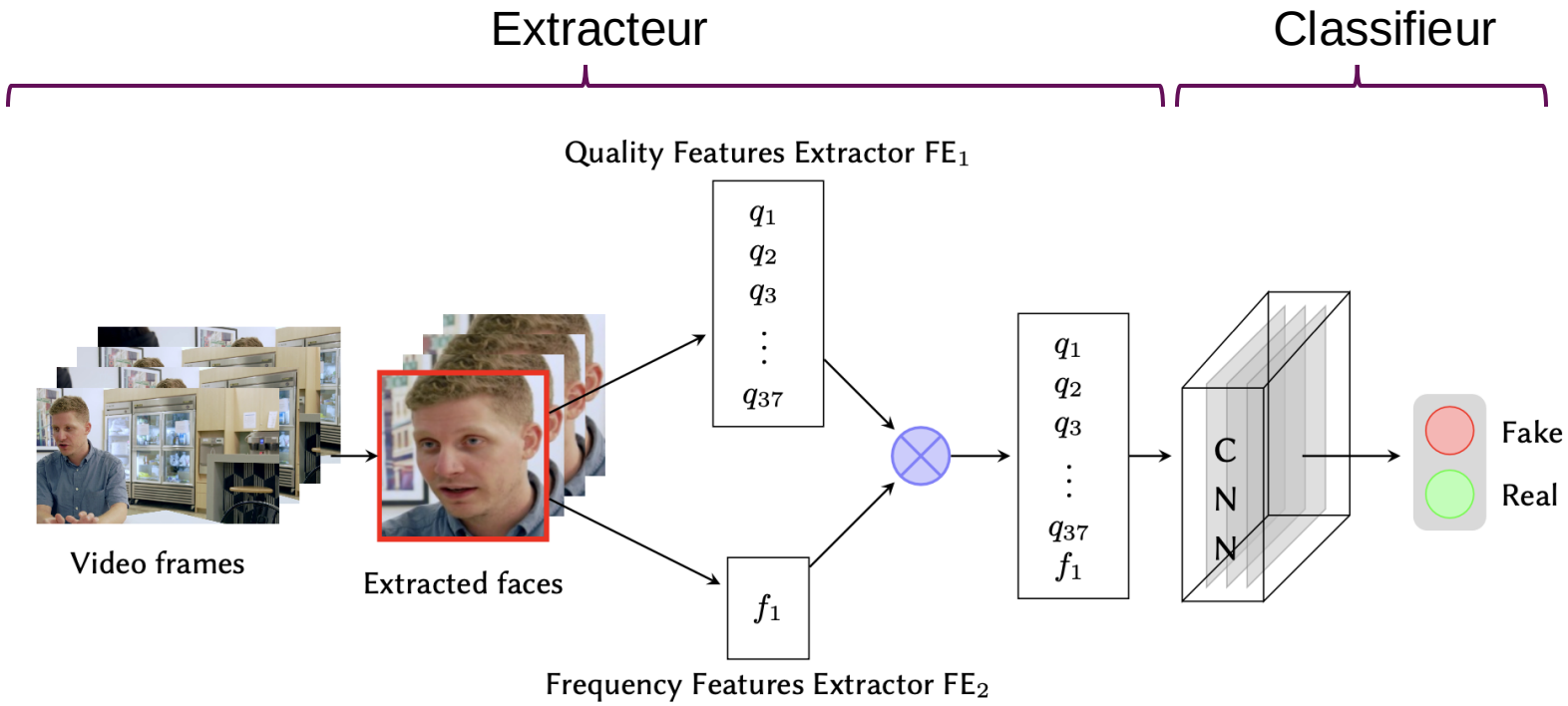


Real Fake

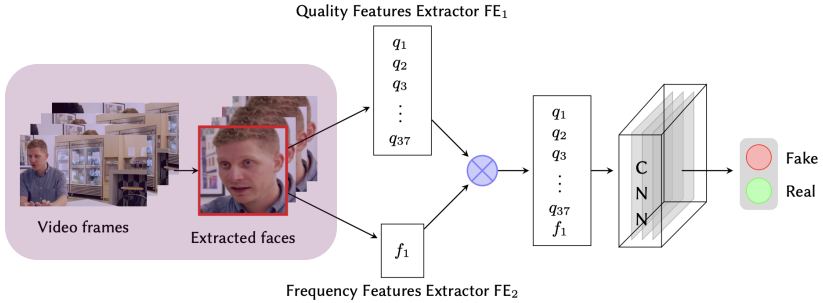
Real Fake

Détection de Deepfake : l'approche proposée

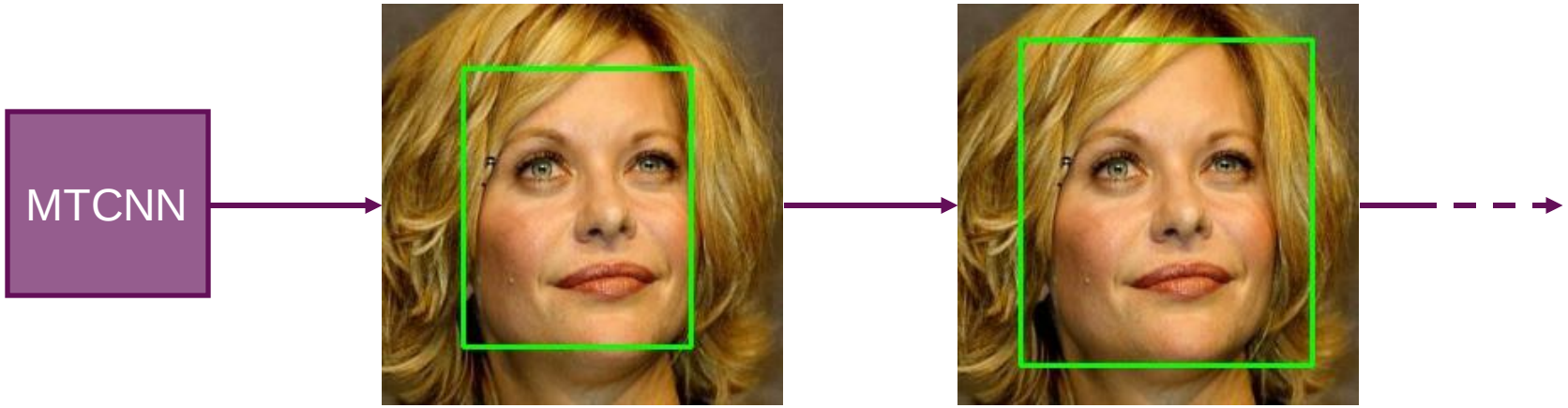
1. Objectif : architecture légère où toutes les caractéristiques utilisées peuvent être expliquées.
   - Architecture classique en deux parties



Détection de Deepfake : la détection du visage

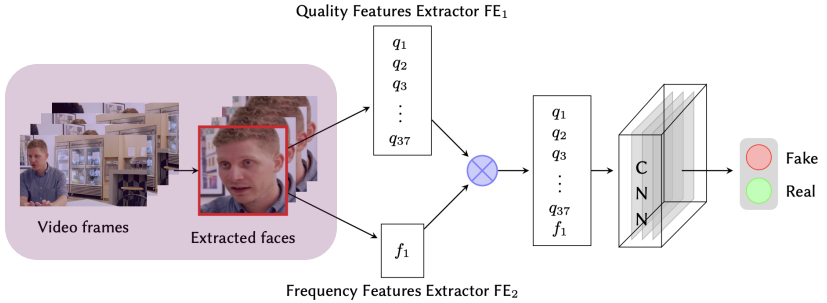


- MTCNN utilisé pour détecter le visage
  - Étant donné que les artefacts apparaissent dans une zone plus large autour du visage, une marge autour du visage est appliquée



Détection de Deepfake : la détection du visage

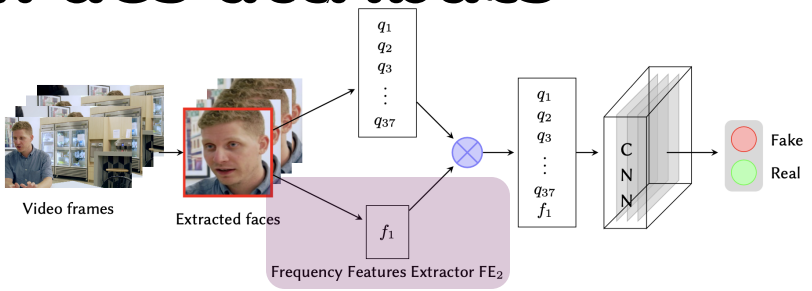
1. Attributs de qualité

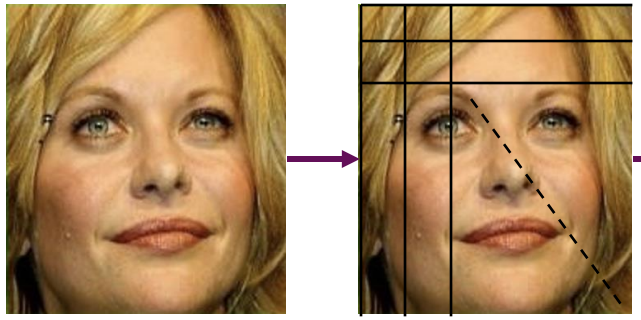


37 attributs

Détection de Deepfake : l'extraction des attributs

2. Analyse fréquentielle





n x *n* blocks

DCT locale

DC	C_{12}	C_{13}	C_{14}	C_{15}
C_{21}	C_{22}	C_{23}	C_{24}	C_{25}
C_{31}	C_{32}	C_{33}	C_{34}	C_{35}
C_{41}	C_{42}	C_{43}	C_{44}	C_{45}
C_{51}	C_{52}	C_{53}	C_{54}	C_{55}

DC	C_{12}	C_{13}	C_{14}	C_{15}
C_{21}	C_{22}	C_{23}	C_{24}	C_{25}
C_{31}	C_{32}	C_{33}	C_{34}	C_{35}
C_{41}	C_{42}	C_{43}	C_{44}	C_{45}
C_{51}	C_{52}	C_{53}	C_{54}	C_{55}

$$r_1 = \frac{\sigma|F|}{\mu|F|}$$

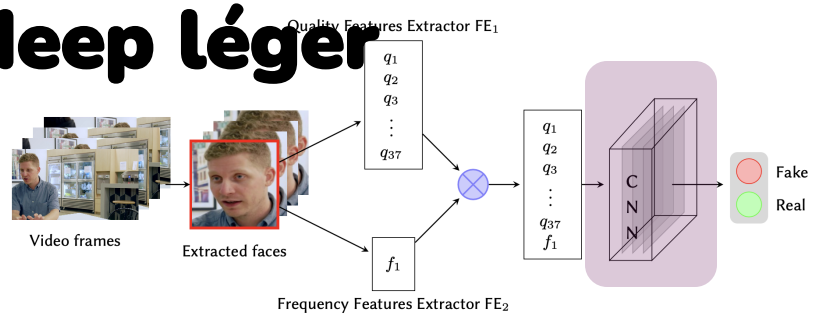
$$r_m = \frac{\sigma|F|}{\mu|F|}$$

coefficients de variation de fréquence

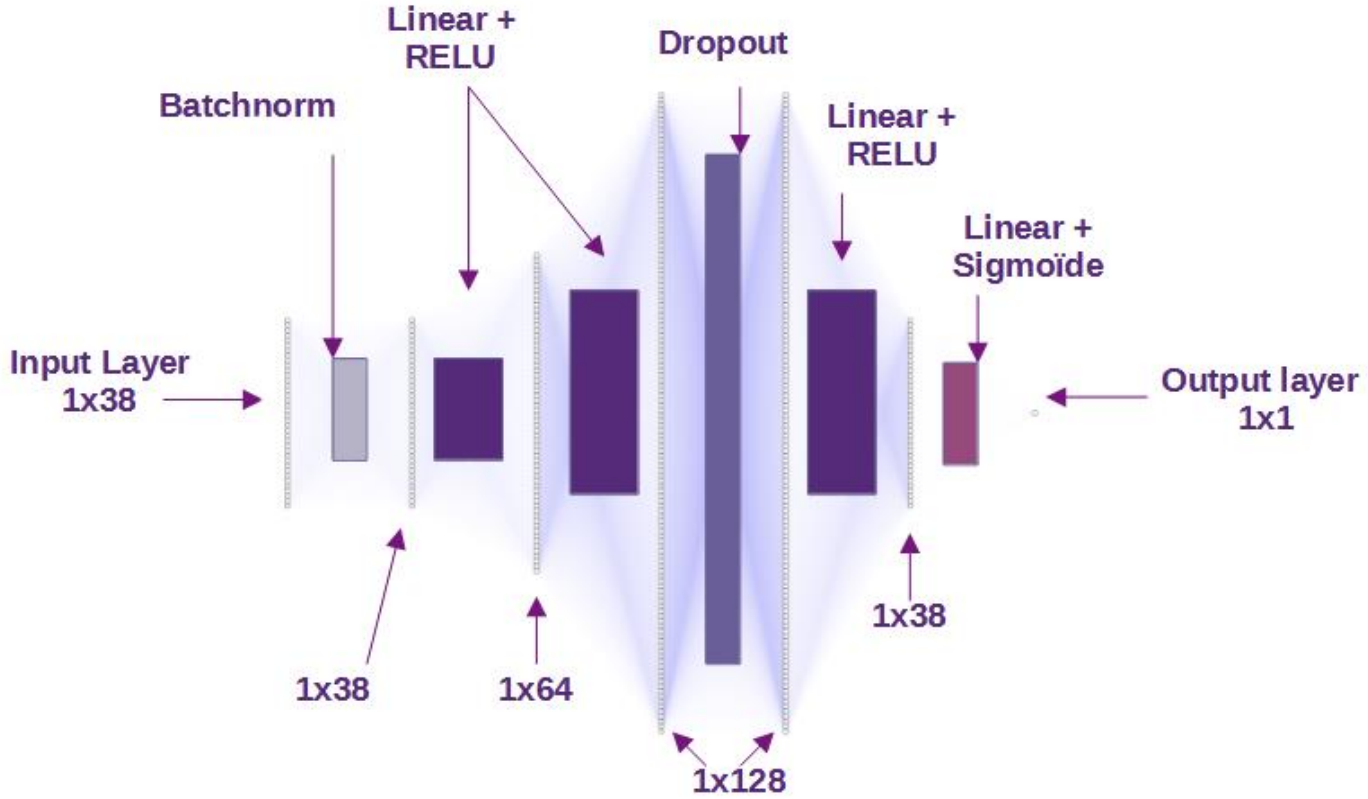
A Z

Moyenne du 10è precentile le plus élevé

Approche proposée : classifieur deep léger



- Principalement basé sur une succession de couches linéaires et d'activations RELU



Experimental setup

- Quatre bases de l'Etat de l'art
  - VidTIMIT
  - DeepFakeTIMIT
  - FF++
  - Celeb-DF

Echantillons de la base DeepFakeTIMIT

- Génération d'une base contenant des vidéos choisies aléatoirement tel que
  - 300 videos réelles de VidTIMIT,
  - 320 Fake videos de DeepFakeTIMIT,
  - 200 réelles and 600 fake videos de FF++,
  - 50 réelles and 50 fake videos de Celeb-DF

} 79 385 réelles et 85 826 fake frames

Experimental setup

- Génération de quatre sous-ensembles à partir de 79 385 réelles et de 85 826 fakes frames
- Sélection aléatoire des frames pour
  - **Training set** avec **31,627 réelles** et **34,826 fake**
  - **Validation set** avec **13,474 réelles** et **15,629 fake**
  - **Test set** avec **13,590 réelles** et **14,466 fake**
  - **Generalization set** avec **20,694 réelles** et **20,905 fake**

Experimental setup

- Critères de performance retenus
  - **Accuracy**
    Fraction des prédictions correctement identifées par le modèle
  - **Recall**
    Pourcentage de positifs correctement prédits par le modèle
  - **Precision**
    Nombre de prédictions positives faites par le modèle.
  - **F1-score**
    moyenne harmonique; fournit une évaluation relativement précise de la performance du modèle.
  - **AUC**
    Performance globale du système

- Modèles de l'état de l'art
  - Xception,
  - DSP-FWA
  - EffiientNetB4
  - EfficientNetB4ATTST

Résultats

- Performance de l'approche proposée

Set	Acccuracy	F1	AUC	Precision	Recall
Train	0.96	0.96	0.99	0.97	0.95
Validation	0.82	0.84	0.88	0.83	0.86
Test	0.84	0.85	0.89	0.83	0.87
Generalization	0.49	0.60	0.52	0.50	0.75

- Comparison avec techniques de l'État de l'art

	Xception	DSP-FWA	EfficientNetB4	EfficientNetB4ATTST	Ours
Accuracy	0.80	0.70	0.98	0.69	0.84
F1	0.85	0.83	0.89	0.72	0.85
AUC	0.87	0.88	0.92	0.82	0.89

- Nombre de paramètres entrainables

	Xception	DSP-FWA	EfficientNetB4	EfficientNetB4ATTST	Ours
Size	22,855,952	25,636,712	19,341,616	21,995,642	16,730

DETECTION DE DEEPFAKE

Contribution :

1. Approche hybride entre les méthodes d'investigation numérique traditionnelles et les méthodes de détection de deepfake les plus modernes
2. Architecture légère, rapide à former et à utiliser
3. Caractéristiques explicables

CONCLUSION

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

PREMIERS RESULTATS

Tutoriaux

- E. Giguet, C. Rosenberger, “Digital Forensics“, Norwegian CyberSecurity Winter School, 2022
- C. Charrier, “Deepfake generation and detection“, Norwegian CyberSecurity Winter School, 2022

Publications

- H. Jean, E. Giguet, C. Charrier, "Video Forgery Detection by Bitstream Analysis", Colour and Visual Computing Symposium Gjøvik - Norway, 2022
- A. Dubettier, T. Gernot, E. Giguet, C. Rosenberger, “File Type Identification Tools for Digital Investigations”, Elsevier Journal on Forensic science : digital investigation, 2023
- S. Cardoso, H. Jean, M. Cherrier, A. Dubettier, T. Gernot, E. Giguet, C. Rosenberger, “Towards an Open-source Digital Investigation Platform”, Cyberworlds 2023
- A. Dubettier, T. Gernot, E. Giguet, C. Rosenberger, “A Comparative Study of Tools for Explicit Content Detection in Images”, Cyberworlds 2023
- H. Jean, C. Rosenberger, E. Giguet, “Sexual explicit content detection in video and audio”, CORESA 2023
- P. Tessé, C. Charrier, E. Giguet, “Contribution des signaux résiduels pour la détection de la permutation de visages dans les vidéos hypertruquées”, CORESA 2023
- P. Tessé, C. Charrier, E. Giguet, “Contribution of residual signals to the detection of face swapping in deepfake videos”, Colour and Visual Computing Symposium Gjøvik - Norway, 2024

Forensic Science International: Digital Investigation 48 (2023) 301574

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

File type identification tools for digital investigations

Adrien Dubettier, Tanguy Gernot, Emmanuel Giguet, Christophe Rosenberger*

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000, Caen, France

ARTICLE INFO

Article history:
Received 23 March 2023
Received in revised form
24 May 2023
Accepted 27 May 2023
Available online xxx

Keywords:
Digital forensics
Digital evidence assessment
Comparative evaluation of forensics tools
Benchmarking
File type identification
File systems

ABSTRACT

Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence for investigation purposes. Building or using file analysis tools is of great interest for a forensic expert to collect high-level information in a short time. In this paper, we consider the examination of files contained in digital media, especially files with possible incorrect types. This often reveals a simple way to hide sensitive content such as porn images, passwords, or accounts. Many commercial and free forensic tools are available for file type identification (FTI). In this work, we assess the performance of ten of them on two significant datasets and scenarios. The main issue we address is the relevance of the tools for forensic purposes. The underlying question is: do expectations meet reality? Our experiments highlight the significant disparity in the accuracy and behavior of the studied tools.

© 2023 Elsevier Ltd. All rights reserved.

1. Introduction

The scope of Digital Forensics covers the application of forensically sound technologies and methods that deal with the recovery, the investigation, the analysis and the reporting on digital materials and digital traces stored in electronic devices. While Digital Forensics has been raised in the late twentieth century with the increasing prevalence of digital technologies for conducting criminal activities (Caviglione et al., 2017), its scope is now extended to legal activities including Art and Cultural Heritage where digital devices may contain material and traces related to the authors, their work, their creation process, their correspondence (Kirschenbaum et al., Donahue; Dietrich and Adelstein, 2015; Jarbrink). Whatever the field of application of Digital Forensics, investigative technologies and tools must meet reliability and accuracy requirements (Flandrin et al., 2014). Their performance should be assessed in terms of speed, but also in terms of accuracy, using well-defined formal assessment procedures, in a way to reinforce trust (Bhat et al., 2021; Lazaridis et al., 2016). This is precisely one of the objectives of Digital Forensic Science: contributing to the professionalization of Digital Forensics by providing objective and independent evaluation protocols in order to lead to reproducible results (Horsman, 2019; Casey, 2019; Dimpe and Kogeda, 2019). This aim leads to define evaluation protocols, with explicit guidelines, clear evaluation metrics, and dedicated datasets.

In an operational context, a forensic expert needs to use one or more tools to quickly process files stored in a device. Many commercial off-the-shelf (COTS) products are proposed and many free open-source software are also candidates for this task. It is often difficult to choose the appropriate tools considering performance (computation time), accuracy, cost and usability. These criteria have to be qualified through a rigorous protocol. Furthermore, it is now popular *to blend the models*, that is to combine the output of different solutions to produce a more robust classifier.

In this article, we are interested in the comparative evaluation of file type identification (FTI) tools. After the forensic acquisition process, which includes device write-blocking, device identifier recording and bit-by-bit imaging, determining file types is one of the first investigation processes carried by investigators at an early stage. With the ever-growing need for data storage which leads to increasingly large storage devices, mining the content of disks requires the use of automated tools. In fact, the investigator has to consider devices ranging from one USB stick, to smartphones, laptops, personal computers, hard drives, and terabytes of server disk drives, in order to recover information or to search for evidence (Beckett and Slay, 2007). Automatically determining file types permits to get a quick overview of the storage device content, sorted or filtered by file categories (e.g. office documents, photos, videos, mailboxes), in order to help the investigator (Sindhu and

* Corresponding author.
E-mail address: christophe.rosenberger@ensicaen.fr (C. Rosenberger).

https://doi.org/10.1016/j.fsidi.2023.301574
2666-2817/© 2023 Elsevier Ltd. All rights reserved.

BILAN

Résultats :

- Qualification d'outils forensiques
- Des premières publications scientifiques
- Cours Forensique créé à l'UNICAEN (Master Informatique)
- Une première version logicielle fonctionnelle de G'DIP
- Implication de nombreux étudiants et ingénieurs

Sujets abordés

- Analyse de la frappe au clavier sonore
- Détection de fichiers chiffrés
- Description du contenu d'images
- Analyse de fragments de fichiers effacés
- Apprentissage sur données confidentielles
- Géolocalisation par le contenu d'images
- Forensique des capteurs d'image
- Altérations d'images/vidéos
- Analyse forensique textuelle
- Détection hypertrucage vidéos
- Détection altération type de fichier
- Détection explicite image/vidéo

BESOINS - COLLABORATIONS

Objectifs :

- Contribuer à l'investigation numérique avec la vision académique (benchmarking, publications)
- Travailler en partenariat avec les acteurs (formation, recherche, tests, verrous)
- Vous accueillir en Normandie pour une future édition de JFIN ?

Besoins :

- Financement (contrats, thèses, projets collaboratifs)
- Accès à des données réelles et du matériel illégal (volume significatif)
- Recueil de besoins (limites des outils actuels et nouvelles fonctionnalités)
- Acquisition de matériels et licences logicielles
- Interventions (conférences ou cours à l'ENSICAEN ou UNICAEN)

Questions

Laboratoire GREYC- UMR CNRS 6072