Projet II

Forensique chez les fantômes de A à Z

Phok Amélie
Bellet Inès

M1 Informatique
Université de Caen Normandie

22 mai 2024

Sommaire

UNIVERSITÉ CAEN NORMANDIE

Présentation

Analyse théorique

Production d'un état de l'art sur la récupération de données effacées et les outils existants

Analyse pratique

Comparaison des quatres logiciels Encase, Autopsy, OSForensics et Recuva choisis dans l'état de l'art selon un protocole scientifique

UNIVERSITÉ CAEN NORMANDIE

Protocole scientifique - explications

Type de fichiers étudiés :

- .txt
- .png
- .pcv (utilisation de Picocrypt sur le png)

Scénarios pour chaque type :

- Copie 1.5GB, suppression 50%
- Copie 1.5GB, suppression 90%
- Copie 1.5GB, suppression 10%, recopie 2GB
- Copie 1.5GB, suppression 70%, recopie 2GB
- Copie 2.5GB, suppression 10%, recopie 2GB
- Copie 2.5GB, suppression 70%, recopie 2GB

UNIVERSITÉ CAEN NORMANDIE

Protocole scientifique schématisé

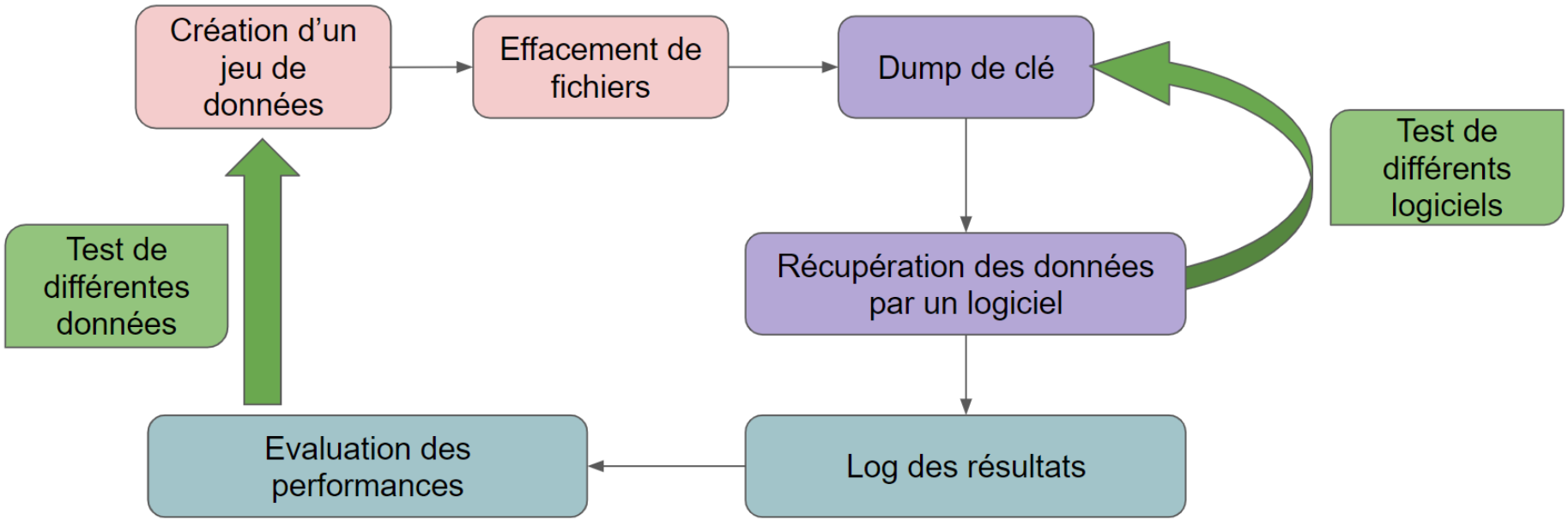


Figure – Schéma du protocole

Manipulations des données : Utilisation de scripts Python et Windows Batch

Clonage du disque : Utilisation de dd pour windows

Fonction de copie

Require: dossier source, nom de la clé, taille en gb

1: **while** la taille voulue n'est pas atteinte **do**
2: **for** chaque fichier du dossier source **do**
3: copier le fichier dans la clé USB
4: **if** le fichier a déja été copié **then**
5: modifier le nom pour indiquer que c'est une copie
6: **end if**
7: **end for**
8: **end while**

Algorithm – Fonction de copie : Amélie

Amelie : copie des fichiers -> base de données < taille clé usb
Ines : base de données >= taille de la clé usb

UNIVERSITÉ CAEN NORMANDIE

Fonction d'effacement

Require: nom clé usb, pourcentage de supression,fichier log, numéro de test
Calculer le nombre de fichiers à supprimer dans la clé pour atteindre le pourecentage de supression voulue
while le nombre de fichier déjà supprimer < nombre fichier à supprimer **do**
tirer au hasard un fichier dans la clé
supprimer le fichier dans la clé
ajouter le fichier dans le log
incrémenté le nombre de fichier déjà supprimer
end while

Algorithm – Fonction de supression : Inès

Amélie : constrution d'une liste avec tirage aléatoire puis suppression + sauvegarde

UNIVERSITÉ CAEN NORMANDIE

Fonction de comparaison

Require: chemin de fichiers_a_copier ,chemin de fichiers_recuperer, numero test, logiciel, type de données
Creer deux listes contenant les fichiers de fichiers_a_copier puis de fichiers_recupere
for chaque fichier f de fichiers_recupere **do**
compare f à celui dans fichiers_a_copier octet à octet
ecrit dans le log s'ils sont identiques ou non
end for

Algorithm – Fonction de comparaison : Inès

UNIVERSITÉ CAEN NORMANDIE

Automatisation

Certaines parties de l'étude prennent beaucoup de temps.
L'automatisation de tâches a donc été utilisée.
Comme nos machines personnelles sont sous Windows, des scripts batch ont été utilisés pour :

- la création des images disques
- l'analyse avec Autopsy car utilisable en ligne de commande
- la comparaison des fichiers récupérés

UNIVERSITÉ CAEN NORMANDIE

Exemple de script batch

```
@echo off
setlocal EnableDelayedExpansion

@REM Script qui construit les dossiers et analyse les images de disques ajoutées en source

:: Paths
set DISK_FOLDER= .\disks
set TIMELOG_FOLDER= .\timelog
set AUTOPSY_BIN= C:\Program Files\Autopsy-4.21.0\bin
set CASE_BASE_DIR= .\autopsy_cases

cd !AUTOPSY_BIN!
:: Iterate through each disk image in the disk folder
for %%f in (%DISK_FOLDER%\"*.img") do (
    :: Extract the filename without the path or extension
    set "FILENAME=%%~nf"

    :: Extract the test number from the filename (assuming filename format is ubs_TESTNUMBER.img)
    for /f "tokens=2 delims=_" %%n in ("%%~nf") do set "TEST_NUMBER=%%n"

    :: Set the case name and case directory
    set "CASE_NAME=test_!TEST_NUMBER!"
    @REM set "CASE_DIR=%CASE_BASE_DIR%\!CASE_NAME!"

    :: Run the Autopsy command and time it
    echo Running Autopsy on !CASE_NAME! ...

    call .\timecmd.bat !AUTOPSY_BIN!\autopsy64.exe --createCase --caseName="!CASE_NAME!"
    --caseBaseDir=%CASE_BASE_DIR% --addDataSource --dataSourcePath="%%f" --runIngest
    --generateReports --console suppress > %TIMELOG_FOLDER%\!TEST_NUMBER!_time.log"

)

echo All done!
endlocal
```

UNIVERSITÉ CAEN NORMANDIE

OSForensics et Recuva

OSForensics :

- Produit commercial (licence temporaire)
- Beaucoup d'outils criminalistique numérique
- Logiciel rapide + efficace
- NTFS $I30
- systeme de note
- Moyenne : 42.02% de fichiers inctats récupérer

Recuva :

- version gratuite
- Simple à utiliser mais pas de mémoire des affaires et des configurations
- Logiciel rapide
- Moyenne : 43.53% de fichiers inctats récupérer

UNIVERSITÉ CAEN NORMANDIE

OSForensics

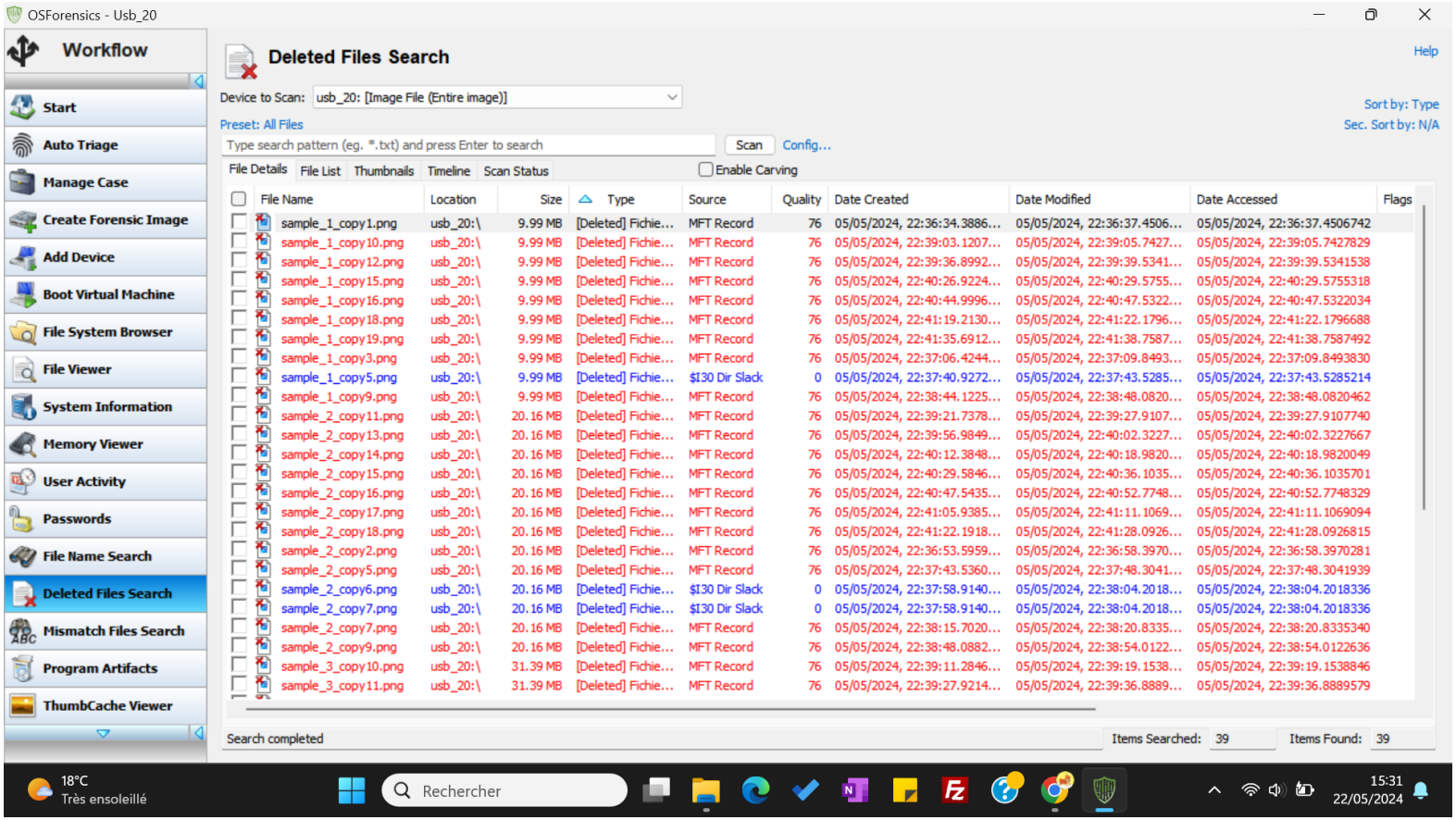


Figure – OSForensic : File details

Recuva

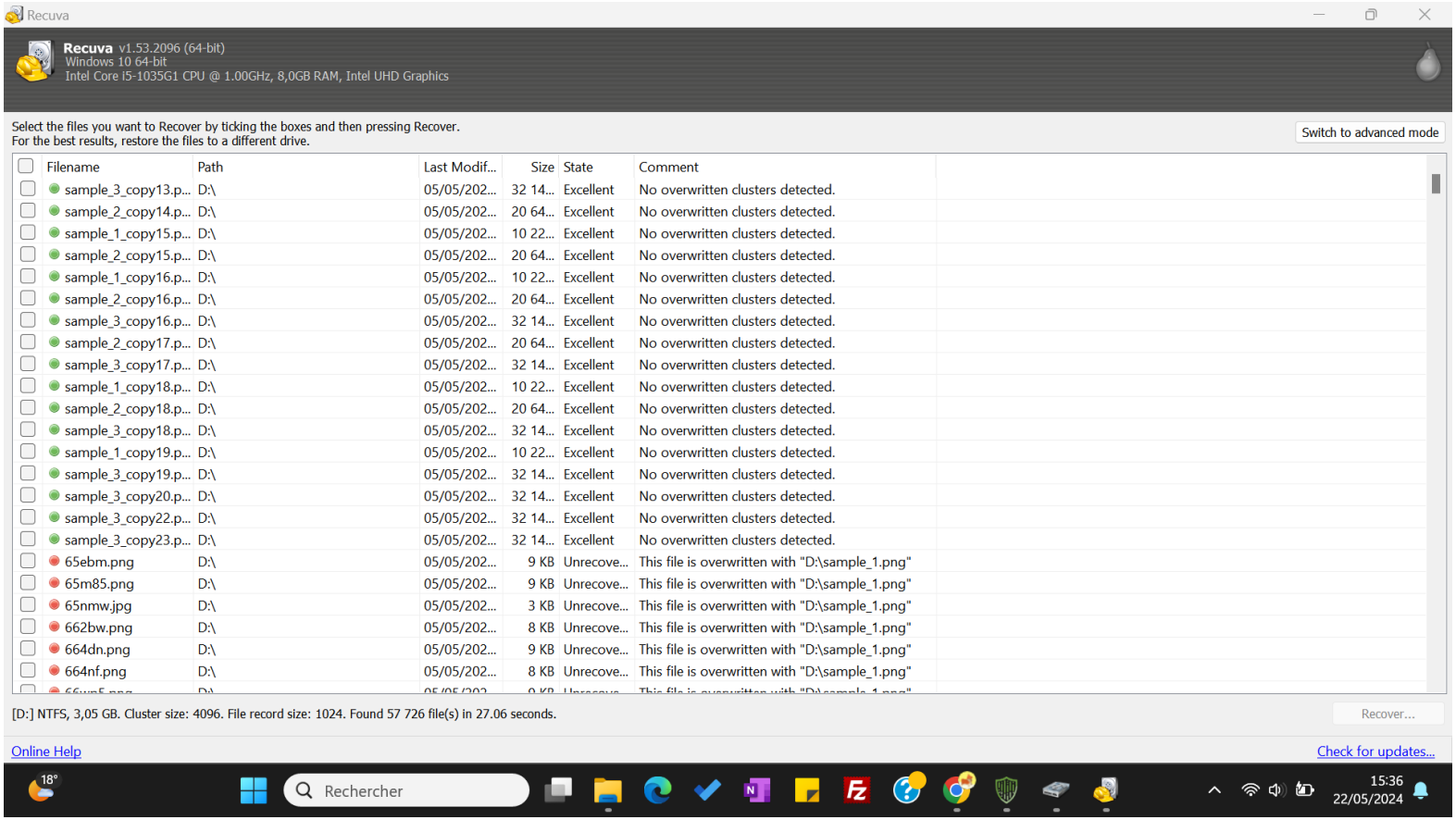


Figure – Recuva

Autopsy et Encase Forensic

Autopsy :

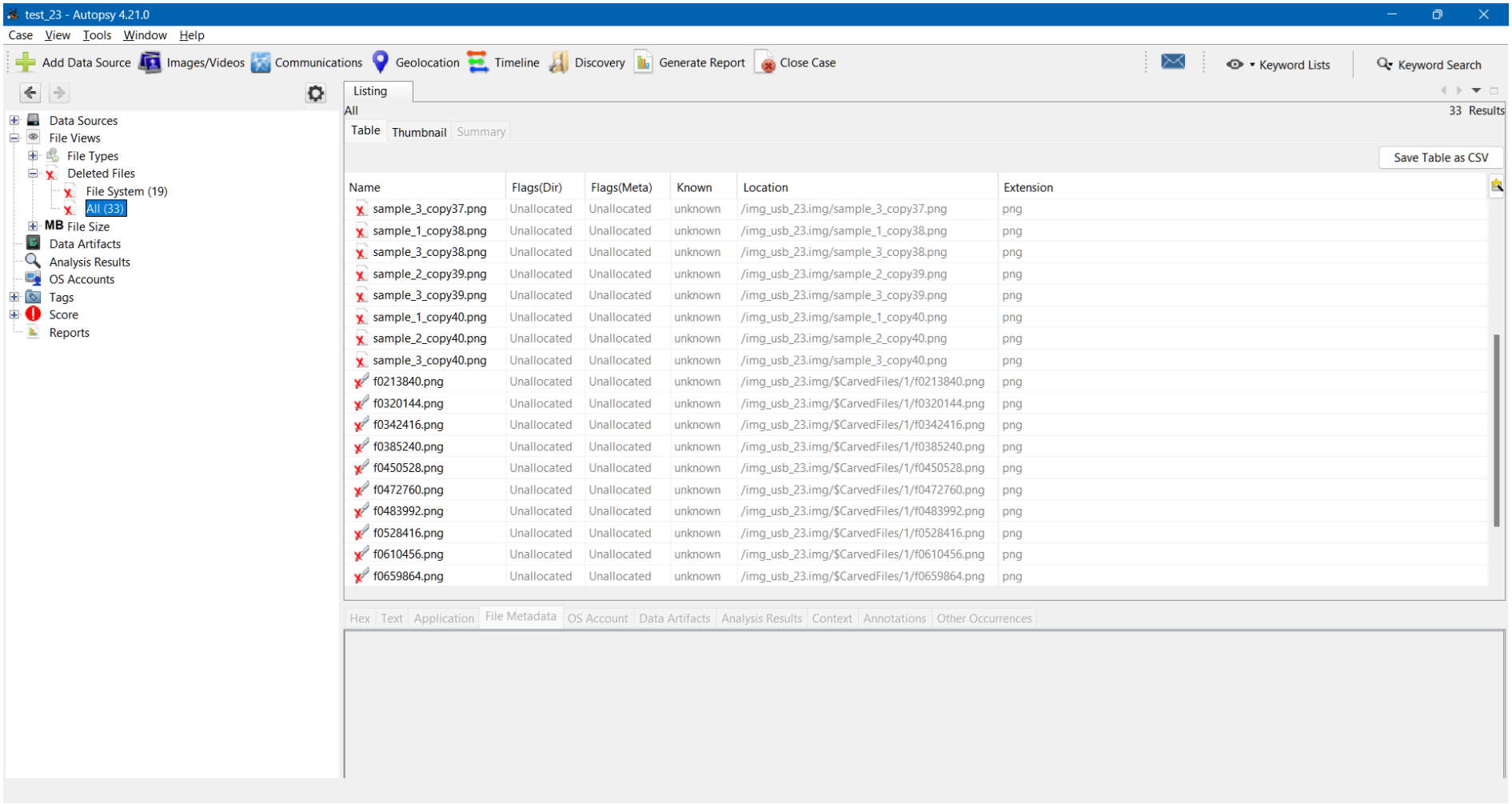
- Logiciel open source
- Logiciel plus lent mais consistant
- Ligne de commande
- Performant dans la récupération
- Moyenne : 53.54% de fichiers intacts lors de la récupération

Encase Forensics :

- Logiciel commercial - licence temporaire de 30 jours
- Pas intuitif mais rapide
- Efficace dans le cas d'un simple effacement
- Moyenne : 45.76% de fichiers intacts lors de la récupération

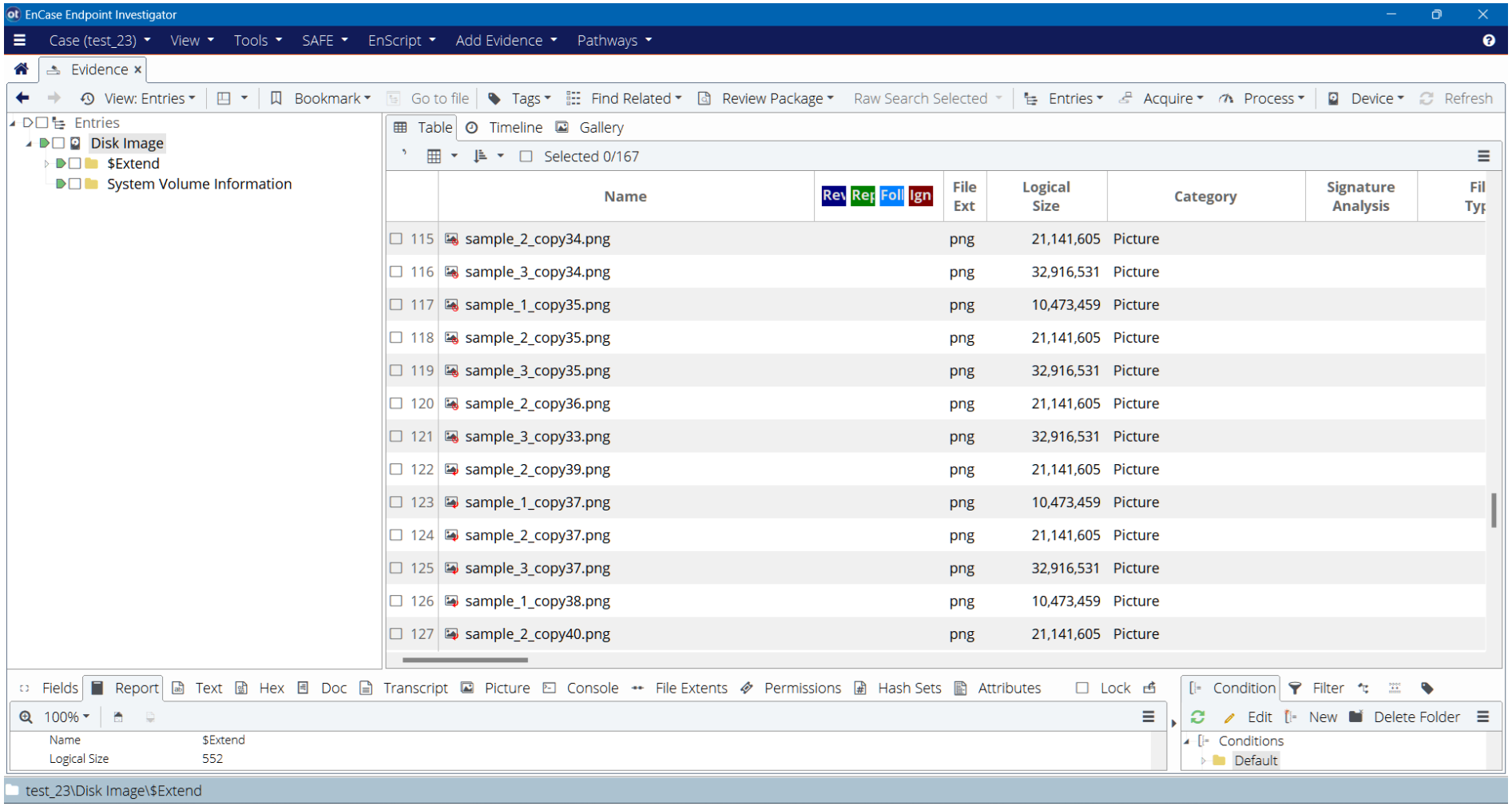
UNIVERSITÉ CAEN NORMANDIE

Autopsy



UNIVERSITÉ CAEN NORMANDIE

Encase Forensics



Expérimentation : Résultat

Performance en temps d'exécution

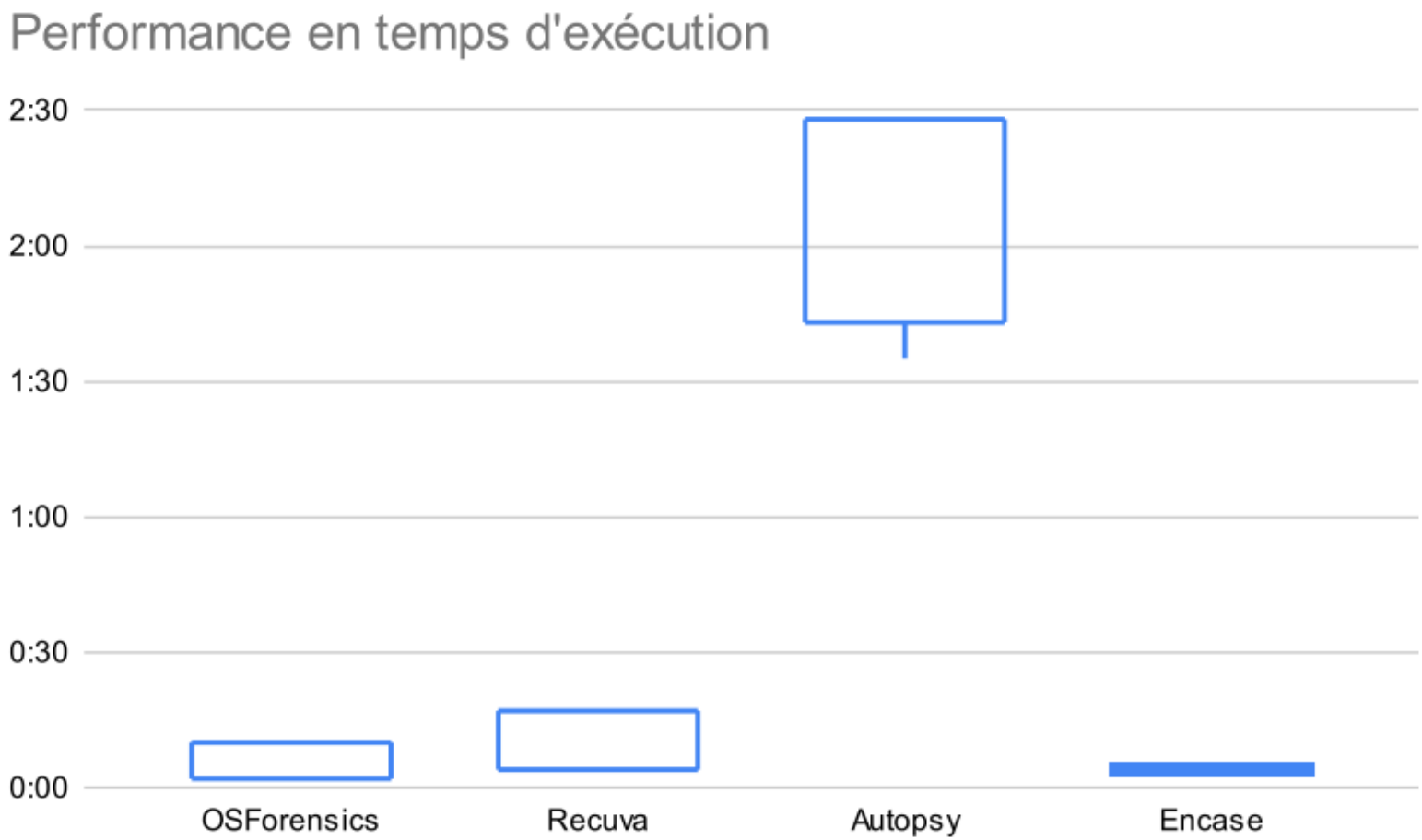
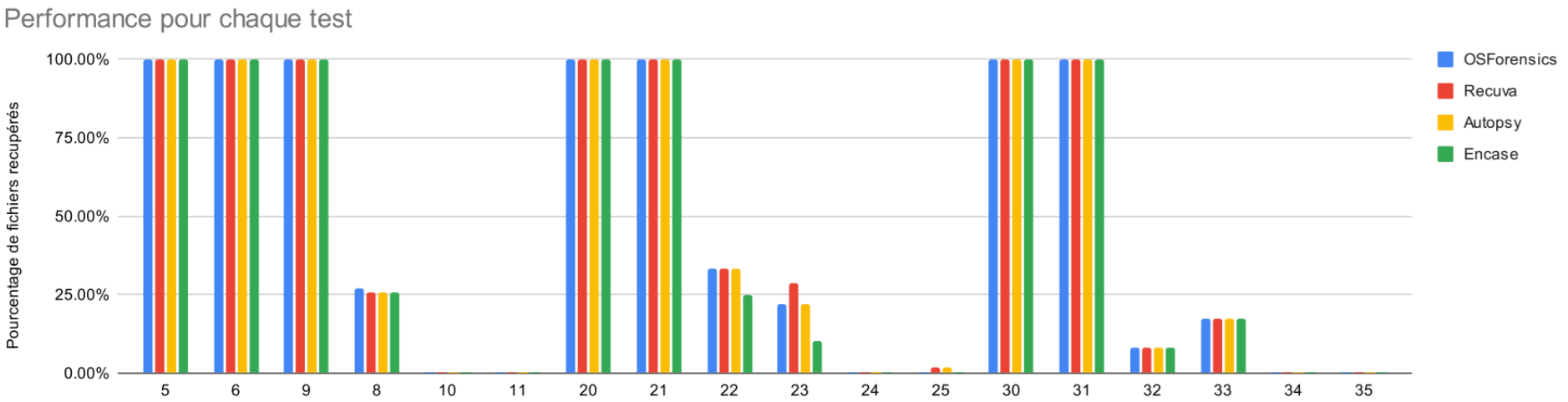


Figure – Performance en temps

Expérimentation : Résultat

Fichiers récupérés



- 5 à 11 : .txt
- 20 à 25 : .png
- 30 à 35 : .pcv

Expérimentation : Résultat

Fichiers intacts

	5	6	9	8	10	11
OSForensics	90.00%	88.46%	95.36%	21.07%	0.00%	0.00%
Recuva	100.00%	100.00%	100.00%	29.86%	0.00%	0.00%
Autopsy	100.00%	100.00%	100.00%	22.99%	0.00%	0.00%
Encase	100.00%	100.00%	100.00%	100.00%	0.00%	0.00%

	20	21	22	23	24	25
OSForensics	75.00%	68.18%	0.00%	31.57%	0.00%	0.00%
Recuva	75.00%	68.18%	0.00%	24.00%	0.00%	0%
Autopsy	100.00%	100.00%	0.00%	47.37%	0.00%	50.00%
Encase	50.00%	50.00%	50.00%	73.68%	0.00%	0.00%

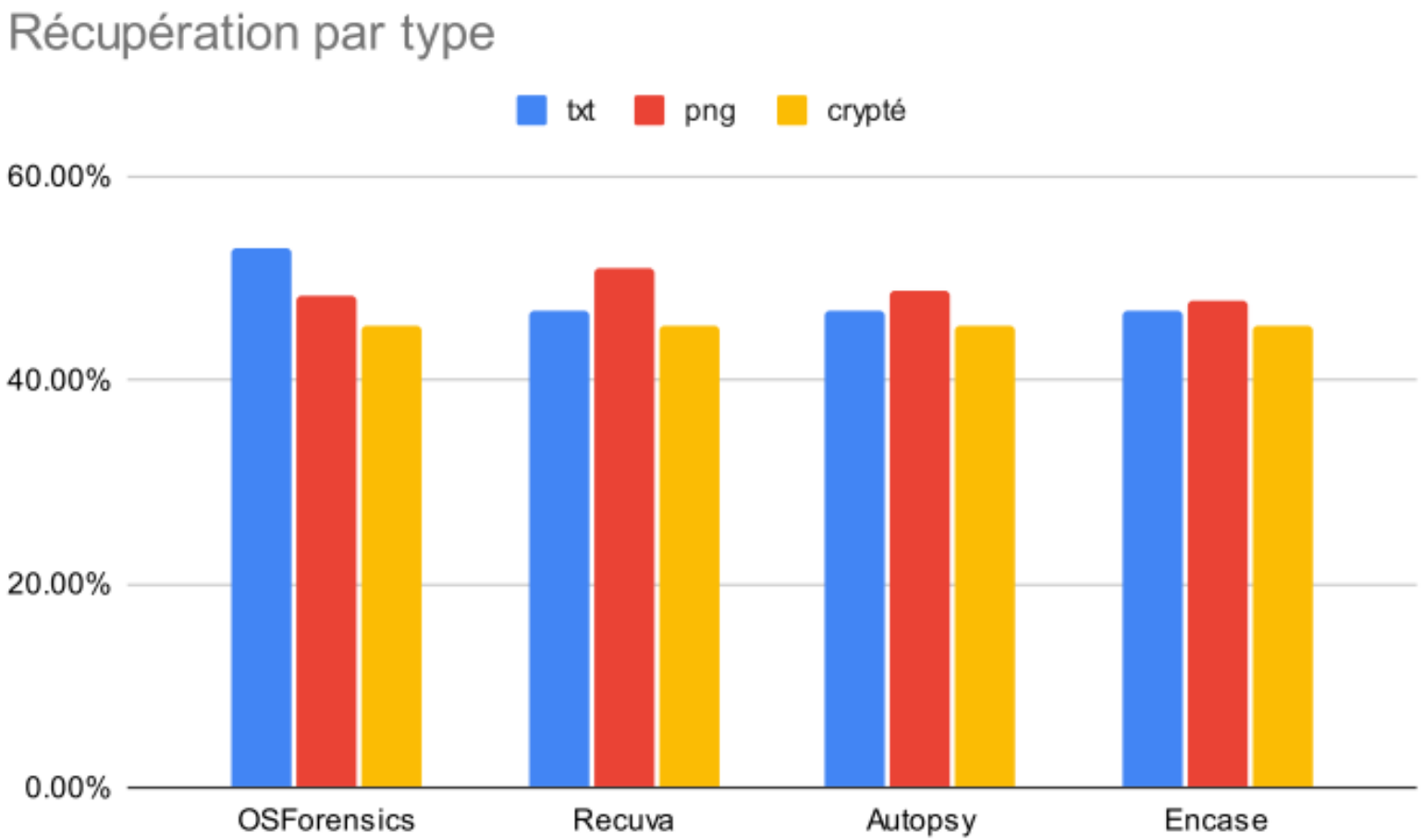
	30	31	32	33	34	35
OSForensics	100.00%	100.00%	0.00%	86.67%	0.00%	0.00%
Recuva	100.00%	100.00%	0.00%	86.67%	0.00%	0.00%
Autopsy	100.00%	100.00%	50.00%	93.33%	0.00%	0.00%
Encase	50.00%	50.00%	50.00%	50.00%	0.00%	0.00%

- 5 à 11 : .txt
- 20 à 25 : .png
- 30 à 35 : .pcv

UNIVERSITÉ CAEN NORMANDIE

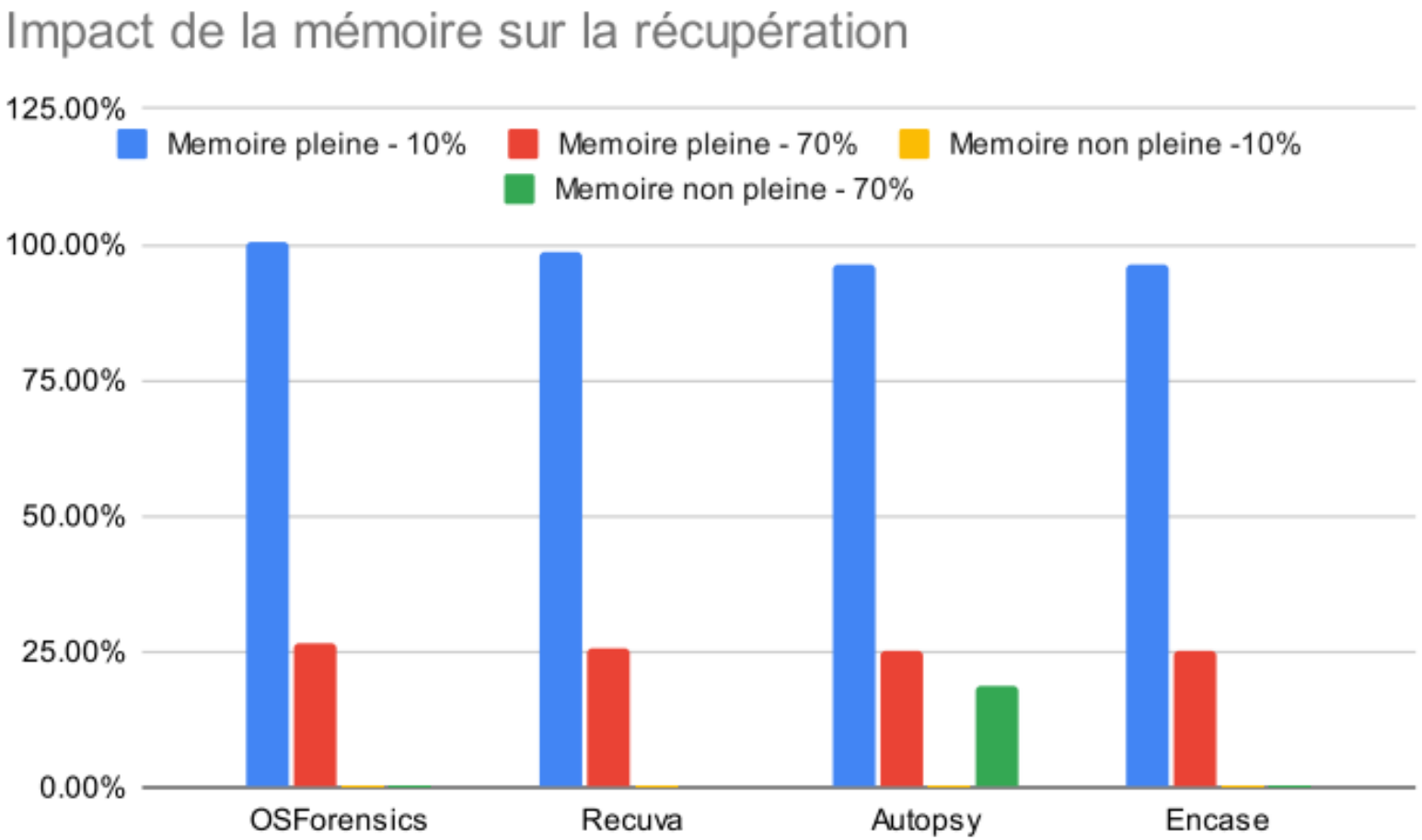
Expérimentation : Résultat

Fichiers récupérés par type



Expérimentation : Résultat

Impact de la mémoire pour la récupération



Conclusion

- OSForensics : performant
- Recuva : facile d'utilisation mais limites sur scénarios complexe
- Autopsy : performant mais temps d'éxécution long
- Encase Forensics : très bon pour fichiers simplement supprimés mais peine apres réécriture + peu maniable

UNIVERSITÉ CAEN NORMANDIE

Propositions d'améliorations

- Augmenter l'automatisation
- Augmenter le corpus de données
- Scénarios plus variés et plus proches de la réalité
- Tester avec davantage de drives (clés usb, HDD, ...)
- Comparaison de coûts entre outils open-source et outils commerciaux
- Formation et documentation pour faciliter l'utilisation des outils
- Tester d'autres outils serait également possible dans une analyse plus approfondie

UNIVERSITÉ CAEN NORMANDIE