

Projet II

Forensique chez les fantômes de A à Z

Phok Amélie
Bellet Inès

M1 Informatique
Université de Caen Normandie

22 mai 2024



- 1 Introduction et présentation du projet
- 2 Protocole scientifique
- 3 Éléments techniques
 - Python
 - Automatisation
- 4 Expérimentation
 - Utilisation des outils
 - Résultats
- 5 Conclusion
- 6 Améliorations

Analyse théorique

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

Analyse pratique

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

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

Protocole scientifique schématisé

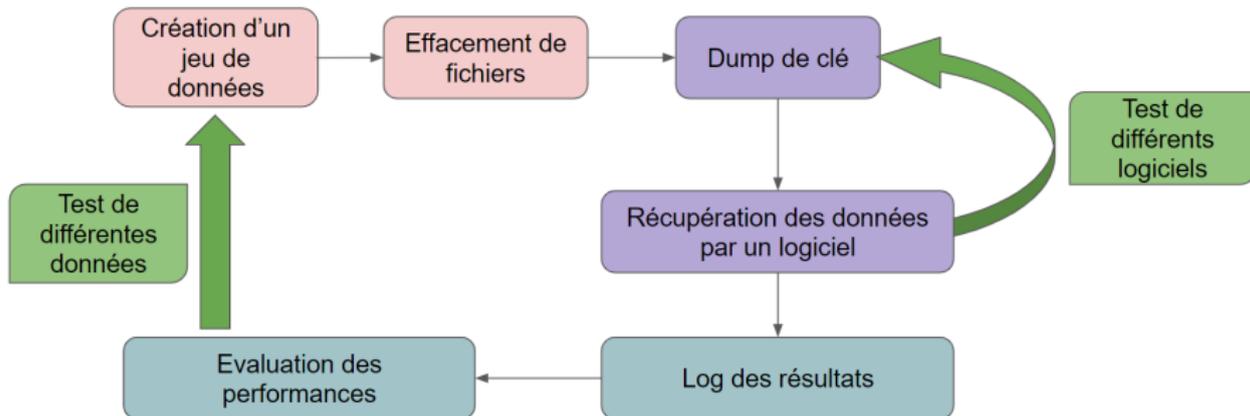


Figure – Schéma du protocole

Manipulations des données : Utilisation de scripts Python et Windows Batch

Clonage du disque : Utilisation de dd pour windows

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 déjà 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

Amélie : copie des fichiers \rightarrow base de données $<$ taille clé usb

Inès : base de données \geq taille de la clé usb

```
Require: nom clé usb, pourcentage de suppression, fichier log, numéro de test  
Calculer le nombre de fichiers à supprimer dans la clé pour atteindre le  
pourcentage de suppression 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 suppression : Inès

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

Fonction de comparaison

```
Require: chemin de fichiers_a_copier ,chemin de fichiers_recuperer, numero test, logiciel, type de données  
Créer 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  
    écrit dans le log s'ils sont identiques ou non  
end for
```

Algorithm – Fonction de comparaison : Inès

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

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 ups_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
```

OSForensics :

- Produit commercial (licence temporaire)
- Beaucoup d'outils criminalistique numérique
- Logiciel rapide + efficace
- NTFS \$130
- système 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

The screenshot displays the OSForensics interface with the 'Deleted Files Search' window open. The search was performed on the device 'usb_20: [Image File (Entire image)]'. The results table shows 39 items found, including files like 'sample_1_copy1.png' and 'sample_2_copy1.png'.

File Name	Location	Size	Type	Source	Quality	Date Created	Date Modified	Date Accessed	Flags
sample_1_copy1.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:36:34.3886...	05/05/2024, 22:36:37.4506...	05/05/2024, 22:36:37.4506742	
sample_1_copy10.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:03.1207...	05/05/2024, 22:39:05.7427...	05/05/2024, 22:39:05.7427829	
sample_1_copy12.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:36.8992...	05/05/2024, 22:39:39.5341...	05/05/2024, 22:39:39.5341538	
sample_1_copy15.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:40:26.9224...	05/05/2024, 22:40:29.5755...	05/05/2024, 22:40:29.5755118	
sample_1_copy16.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:40:44.9996...	05/05/2024, 22:40:47.5322...	05/05/2024, 22:40:47.5322034	
sample_1_copy18.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:41:19.2130...	05/05/2024, 22:41:22.1796...	05/05/2024, 22:41:22.1796688	
sample_1_copy19.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:41:35.6912...	05/05/2024, 22:41:38.7587...	05/05/2024, 22:41:38.7587492	
sample_1_copy3.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:37:06.4244...	05/05/2024, 22:37:09.8493...	05/05/2024, 22:37:09.8493830	
sample_1_copy5.png	usb_20\1	9.99 MB	Deleted; Fichie...	830 Dr Slack	0	05/05/2024, 22:37:40.9272...	05/05/2024, 22:37:43.5285...	05/05/2024, 22:37:43.5285214	
sample_1_copy9.png	usb_20\1	9.99 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:38:44.1225...	05/05/2024, 22:38:48.0820...	05/05/2024, 22:38:48.0820462	
sample_2_copy11.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:21.7378...	05/05/2024, 22:39:27.9107...	05/05/2024, 22:39:27.9107740	
sample_2_copy13.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:56.9849...	05/05/2024, 22:40:02.3227...	05/05/2024, 22:40:02.3227667	
sample_2_copy14.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:40:12.3848...	05/05/2024, 22:40:18.9820...	05/05/2024, 22:40:18.9820049	
sample_2_copy15.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:40:29.5846...	05/05/2024, 22:40:36.1035...	05/05/2024, 22:40:36.1035710	
sample_2_copy16.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:40:47.5435...	05/05/2024, 22:40:52.7748...	05/05/2024, 22:40:52.7748329	
sample_2_copy17.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:41:05.9385...	05/05/2024, 22:41:11.1069...	05/05/2024, 22:41:11.1069904	
sample_2_copy18.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:41:22.1918...	05/05/2024, 22:41:28.0926...	05/05/2024, 22:41:28.0926815	
sample_2_copy2.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:36:53.9959...	05/05/2024, 22:36:58.3970...	05/05/2024, 22:36:58.3970281	
sample_2_copy5.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:37:43.2360...	05/05/2024, 22:37:48.3041...	05/05/2024, 22:37:48.3041939	
sample_2_copy6.png	usb_20\1	20.16 MB	Deleted; Fichie...	830 Dr Slack	0	05/05/2024, 22:37:58.6140...	05/05/2024, 22:38:04.2018...	05/05/2024, 22:38:04.2018336	
sample_2_copy7.png	usb_20\1	20.16 MB	Deleted; Fichie...	830 Dr Slack	0	05/05/2024, 22:37:58.6140...	05/05/2024, 22:38:04.2018...	05/05/2024, 22:38:04.2018336	
sample_2_copy7.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:38:15.7020...	05/05/2024, 22:38:20.8335...	05/05/2024, 22:38:20.8335340	
sample_2_copy9.png	usb_20\1	20.16 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:38:48.0882...	05/05/2024, 22:38:54.0122...	05/05/2024, 22:38:54.0122636	
sample_2_copy10.png	usb_20\1	31.39 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:11.2846...	05/05/2024, 22:39:19.1538...	05/05/2024, 22:39:19.1538846	
sample_2_copy11.png	usb_20\1	31.39 MB	Deleted; Fichie...	MFT Record	76	05/05/2024, 22:39:27.9214...	05/05/2024, 22:39:36.8889...	05/05/2024, 22:39:36.8889579	

Figure – OSForensic : File details

Recuva v1.53.2006 (64-bit)
Windows 10 64-bit
Intel Core i5-1025G1 CPU @ 1.00GHz, 8.0GB RAM, Intel UHD Graphics

Select the files you want to Recover by ticking the boxes and then pressing Recover.
For the best results, restore the files to a different drive.

File name	Path	Last Modified	Size	State	Comment
<input type="checkbox"/> sample_3_copy13.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy14.p...	D:\	05/05/202...	20 64...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_1_copy15.p...	D:\	05/05/202...	10 22...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy15.p...	D:\	05/05/202...	20 64...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_1_copy16.p...	D:\	05/05/202...	10 22...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy16.p...	D:\	05/05/202...	20 64...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy16.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy17.p...	D:\	05/05/202...	20 64...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy17.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_1_copy18.p...	D:\	05/05/202...	10 22...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy18.p...	D:\	05/05/202...	20 64...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy18.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_1_copy19.p...	D:\	05/05/202...	10 22...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy19.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_2_copy20.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy22.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> sample_3_copy23.p...	D:\	05/05/202...	32 14...	Excellent	No overwritten clusters detected.
<input type="checkbox"/> 65ebm.png	D:\	05/05/202...	9 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 65m85.png	D:\	05/05/202...	9 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 65nmw.jpg	D:\	05/05/202...	3 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 662bw.png	D:\	05/05/202...	8 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 664dn.png	D:\	05/05/202...	9 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 664nf.png	D:\	05/05/202...	8 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"
<input type="checkbox"/> 664nf.png	D:\	05/05/202...	8 KB	Unrecover...	This file is overwritten with "D:\sample_1.png"

[D:] NTFS, 3,05 GB, Cluster size: 4096, File record size: 1024, Found 57 726 files (in) in 27,06 seconds.

Online Help Check for updates...

Figure – Recuva

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

test_23 - Autopsy 4.21.0

Case View Tools Window Help

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

Keyword Search 33 Results

Save Table as CSV

Name	Flags(Dir)	Flags(Meta)	Known	Location	Extension
sample_3_copy37.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_3_copy37.png	png
sample_1_copy38.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_1_copy38.png	png
sample_3_copy38.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_3_copy38.png	png
sample_2_copy39.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_2_copy39.png	png
sample_3_copy39.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_3_copy39.png	png
sample_1_copy40.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_1_copy40.png	png
sample_2_copy40.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_2_copy40.png	png
sample_3_copy40.png	Unallocated	Unallocated	unknown	/img_usb_23.img/sample_3_copy40.png	png
f0213840.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0213840.png	png
f0320144.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0320144.png	png
f0342416.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0342416.png	png
f0385240.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0385240.png	png
f0450528.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0450528.png	png
f0472760.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0472760.png	png
f0483992.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0483992.png	png
f0528416.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0528416.png	png
f0610456.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0610456.png	png
f0659864.png	Unallocated	Unallocated	unknown	/img_usb_23.img/\$CarvedFiles/1/f0659864.png	png

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

Encase Forensics

The screenshot displays the Encase Endpoint Investigator interface. The main window shows a tree view on the left with 'Disk Image' selected, containing '\$Extend' and 'System Volume Information'. The central pane shows a table of files with columns for Name, File Ext, Logical Size, Category, Signature Analysis, and File Type. The table lists 13 files, all with a '.png' extension and a 'Picture' category. The bottom pane shows a detailed view of the selected file, displaying its name and logical size.

	Name	File Ext	Logical Size	Category	Signature Analysis	File Type
115	sample_2_copy34.png	png	21,141,605	Picture		
116	sample_3_copy34.png	png	32,916,531	Picture		
117	sample_1_copy35.png	png	10,473,459	Picture		
118	sample_2_copy35.png	png	21,141,605	Picture		
119	sample_3_copy35.png	png	32,916,531	Picture		
120	sample_2_copy36.png	png	21,141,605	Picture		
121	sample_3_copy33.png	png	32,916,531	Picture		
122	sample_2_copy39.png	png	21,141,605	Picture		
123	sample_1_copy37.png	png	10,473,459	Picture		
124	sample_2_copy37.png	png	21,141,605	Picture		
125	sample_3_copy37.png	png	32,916,531	Picture		
126	sample_1_copy38.png	png	10,473,459	Picture		
127	sample_2_copy40.png	png	21,141,605	Picture		

Expérimentation : Résultat

Performance en temps d'exécution

Performance en temps d'exécution

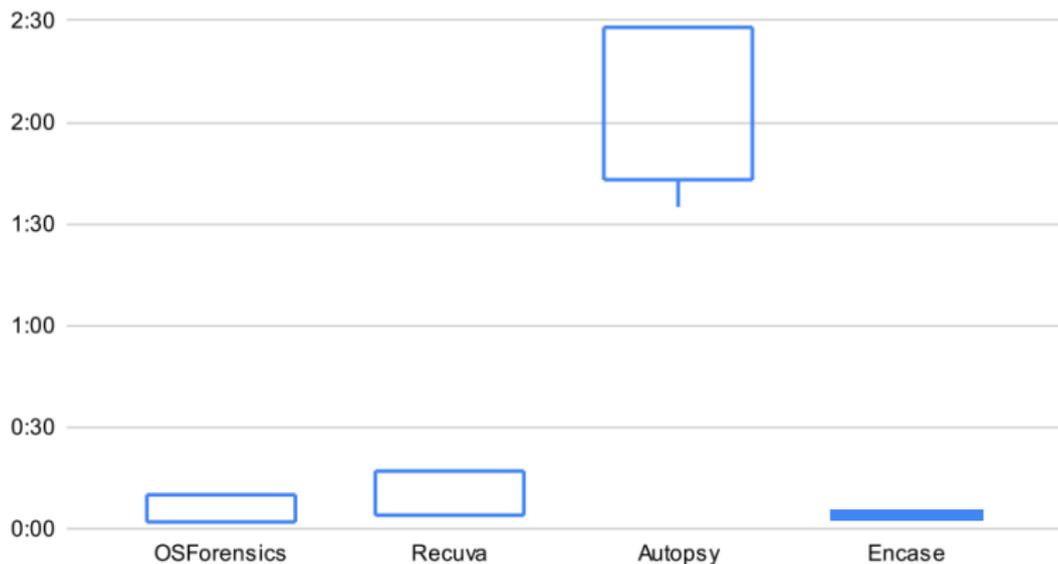
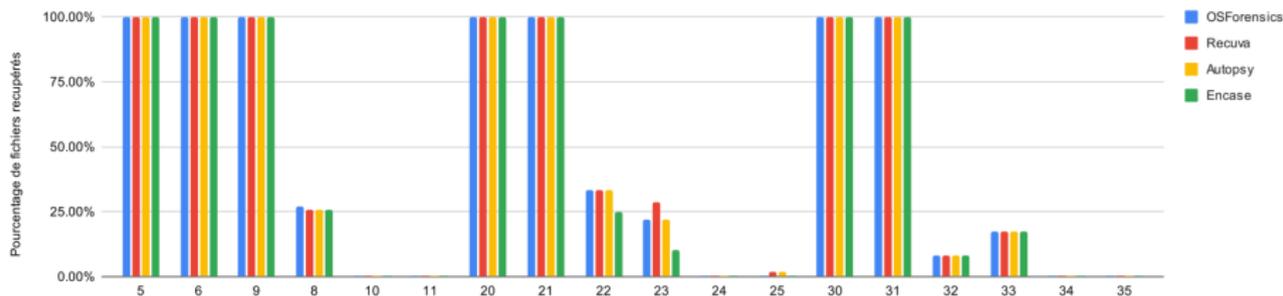


Figure – Performance en temps

Expérimentation : Résultat

Fichiers récupérés

Performance pour chaque test



- 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%

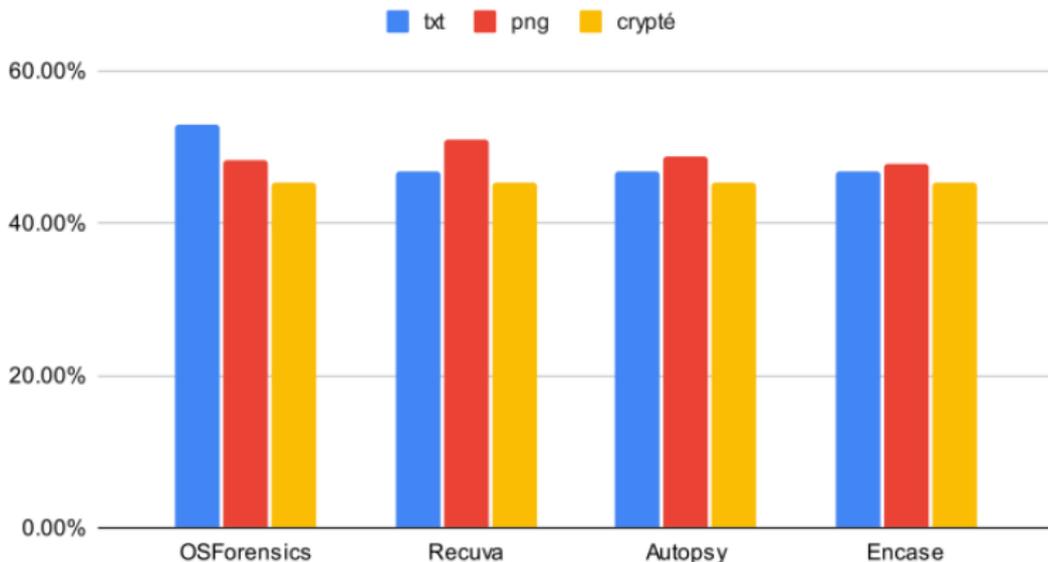
	30	31	32	33	34	35
OSForensics	100.00%	100.00%	0.00%	86.67%	0.00%	0.00%
Recuva	100.00%	100.00%	0.00%	86.67%	0.00%	0.00%
Autopsy	100.00%	100.00%	50.00%	93.33%	0.00%	0.00%
Encase	50.00%	50.00%	50.00%	50.00%	0.00%	0.00%

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

Expérimentation : Résultat

Fichiers récupérés par type

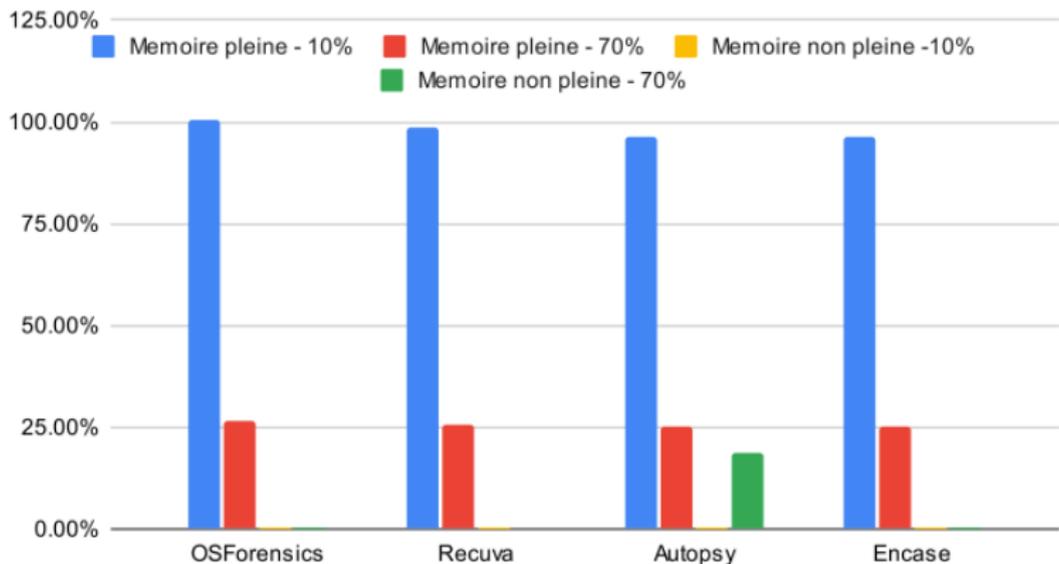
Récupération par type



Expérimentation : Résultat

Impact de la mémoire pour la récupération

Impact de la mémoire sur la récupération



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

- 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