**PARTIE A : PROCEDURE STANDARD AU TELECHARGEMENT DE CONTENU INAPPROPRIE.**

1. **Préparation et Planification**

L’enquête doit être autorisé par le PDG, tenable Lionel, suite à des soupçons d’infractions commises par bob Donovelli, employé de l’entreprise.

1. **Détection d’incident**

L’équipe RH à signaler que bob Donovelli aurait téléchargé du contenue inappropriés depuis son poste de travail. Il est essentiel de vérifier la source de cette information (rapport de la rh, les logs réseau) et de sauvegarder les détails, y compris la date et l’heure

1. **Réponse Initiale**

Dès la détection de l’incident, l’ordinateur de bob doit être isolé du réseau pour empêcher toute altération ou destruction de preuves.

Si l’oridnateur est allumé capturez les données volatiles à l’aide d’outils comme volatility. Notez tous les processus en cours, le site web ouverts, vérifier l’historique de tous les navigateurs, les connexions réseau actives.

1. **Formulation de la stratégie de réponse**

Il est essentiel de déterminer l’objectif de l’enquête.

Identifiez le type d’experts nécessaires pour mener cette enquête. Assurez-vous que les preuves présentées par l’enquêteurs sont admissibles devant un tribunal.

1. **Sauvegarde Forensique**

Effectuez une image du disque dur de bob, utiliser l’outil comme dcfldd pour faire une copie exacte du disque.

Documentez chaque étape, y compris qui à manipuler. Utiliser la chaine de traçabilité

1. **Investigation**

Monter le disque dur en lecture seul pour éviter toute modification. Utiliser autopsy pour analyser les fichiers, l’historique de navigation et les journaux des activités de bob.

Si le système est allumé analyser les données volatiles comme les processus en cours et les page web en mémoire à l’aide de volatility

Si bob utiliser un vpn cela pourrait compliquer l’enquête.

1. **Implémentation des Mesures de sécurité**

Mettre à jour les politiques de filtrage du réseau et renforcez les contrôles de sécurité pour éviter que de tels incidents ne se reproduisent. Sensibilisez les employés sur l’utilisation appropriée des systèmes informatiques.

1. **Contrôle Réseau**

Renforcez la surveillance du réseau pour détecter toute tentative future d’accès à des sites inappropriés. Utiliser des outils comme elk siem, splunk

1. **Récupération**

Une fois l’enquête terminée, remettez l’ordinateur de bob dans son état initial, sans fichier illicites.

1. **Présentation**

Rédiger un rapport complet contenant les preuves collectées, les dates et heures des infractions, ainsi que les méthodes utilisées pour l’enquête. Que vous allez soumettre à la RH et la direction pour qu’ils puissent prendre les mesures légales appropriées contre bob.

1. **Suivi**

Organisez un audit des pratiques de sécurité pour vous assurer que les nouvelles mesures sont respectées. Effectuer une formation pour rappeler aux employés

**PARTIE B : RAPPORT D’ANALYSE FORENSIC CAS D’UN TELECHARGEMENT INAPROPRIE**

Rédiger par NKAMWA Loïc

Date de remise : 13/10/2024

Date de réception : 04/10/2024

Identificateur du cas : 1.0

Identité et signature de l’examinateur : Lionel Tenable

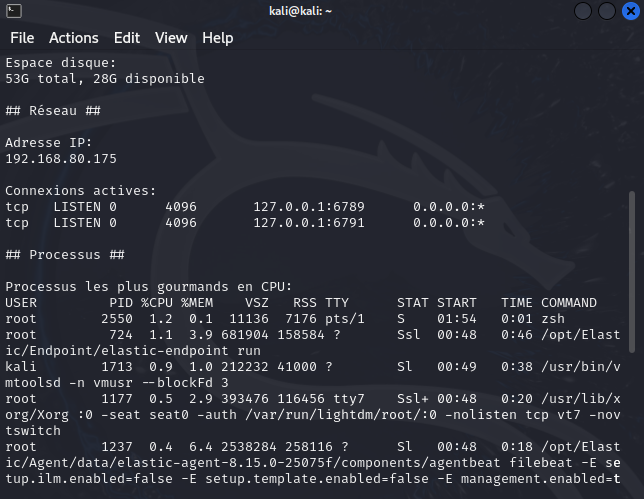
Identité de l’agence faisant le rapport : Saintcyber

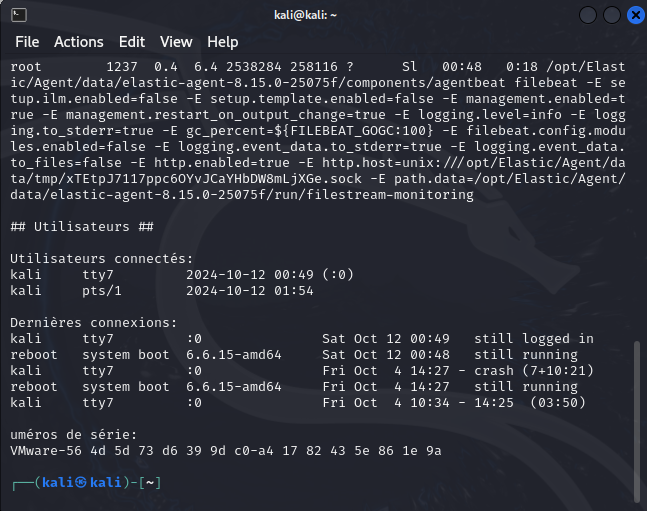
**CAS D’INVESGATION**

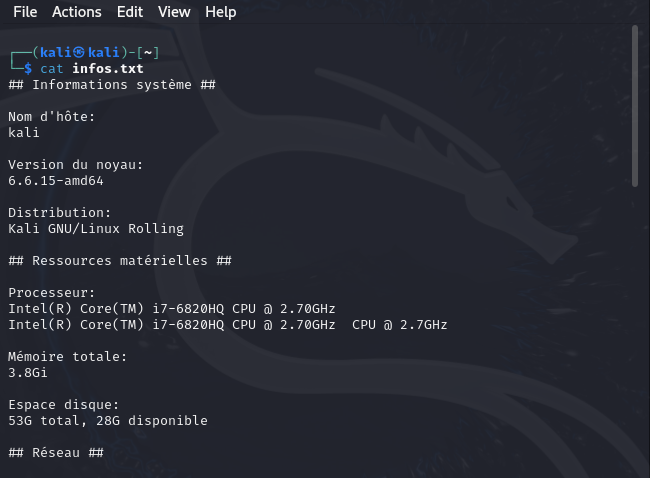
Le service des ressources humaines a été alerté par un rapport interne indiquant que Bob Donovelli aurait accédé à du contenu inapproprié via son poste de travail professionnel. L’enquête a été autorisée par le PDG afin de confirmer ou infirmer ces allégations, en respectant les procédures légales en vigueur.

**DESCRIPTIONS DES ITEMS SOUMIS A L'INVESTIGATION**

1. **PROCEDURE D’ACQUISITION DES PREUVES**

L’ordinateur était allumé au moment de l'intervention, nous avons fait un script qui nous a permis d’obtenir différentes informations sur le pc de bob le 12 octobre 2024 à 00 h :49 min et nous avons obtenu comme information, le numéro de série, les utilisateurs connectés, les processus, l’adresse IP, connexion active. 

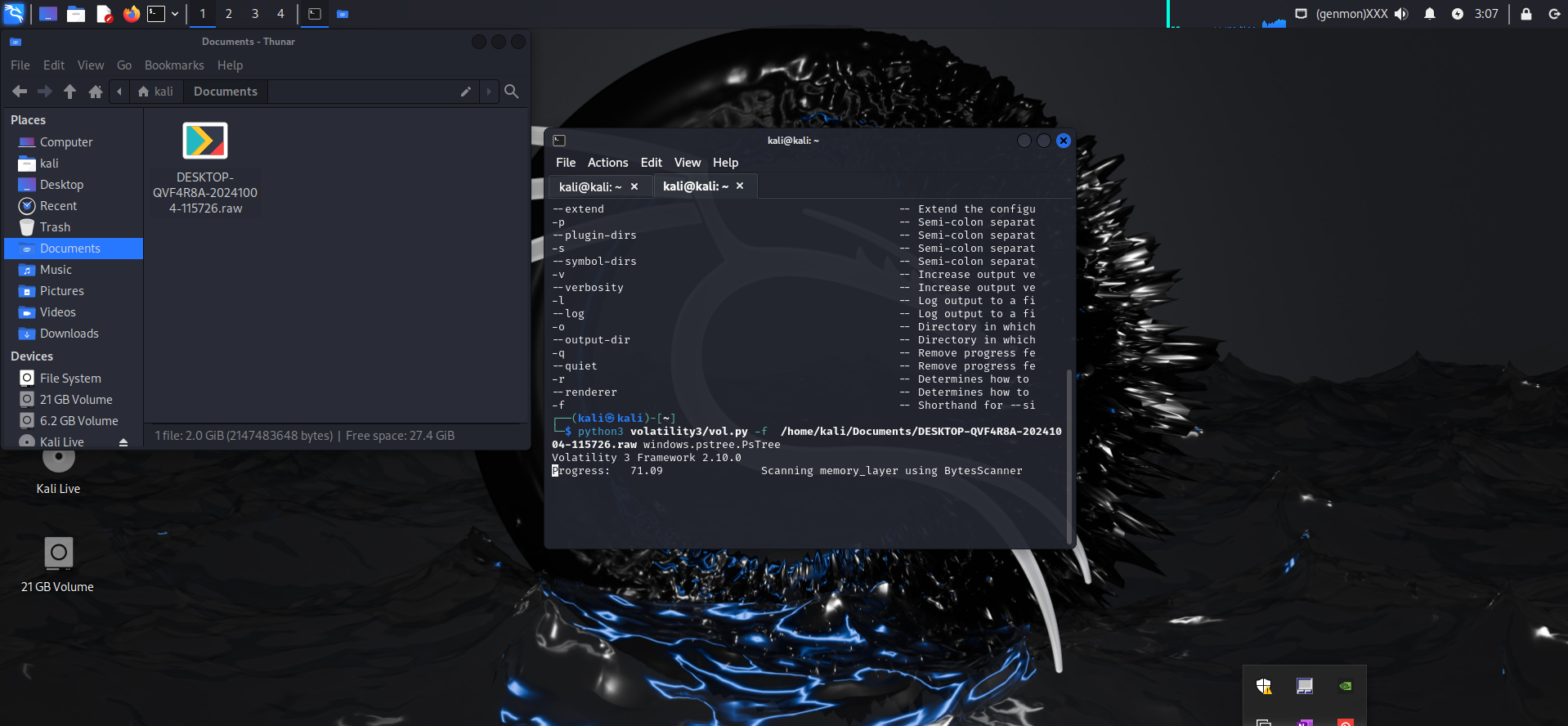




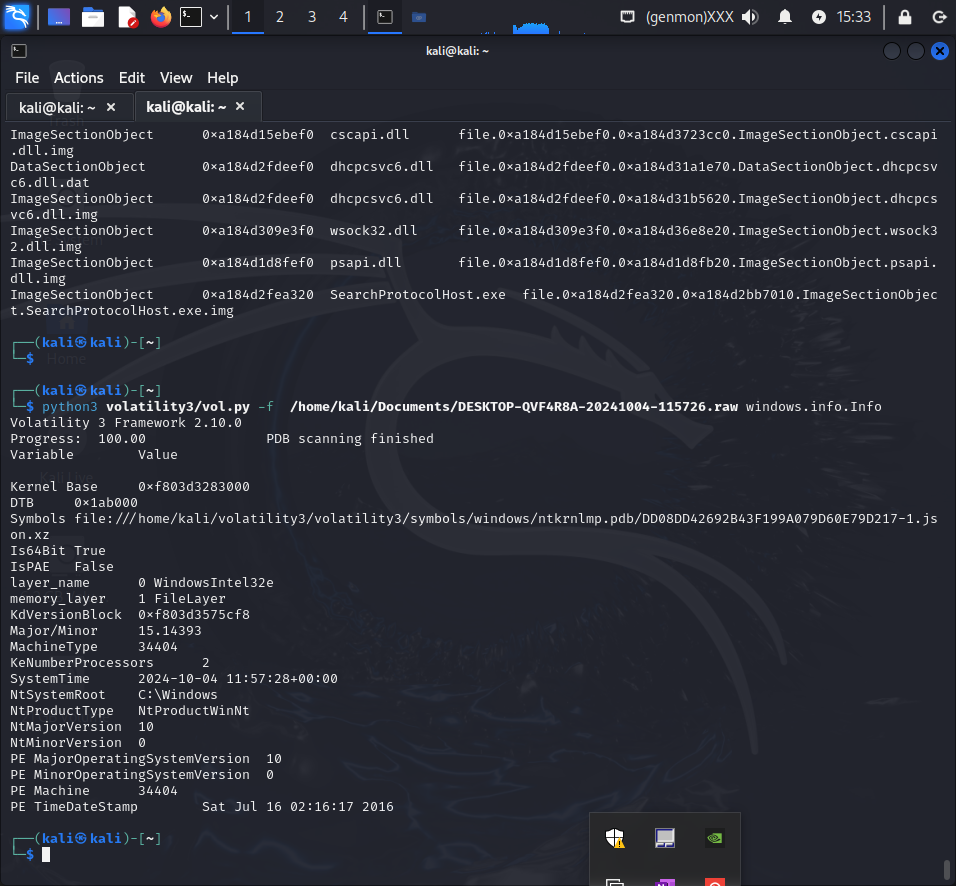
Ces informations ont été documentées y compris la date et l’heure

1. **ANALYSE des Fichiers**

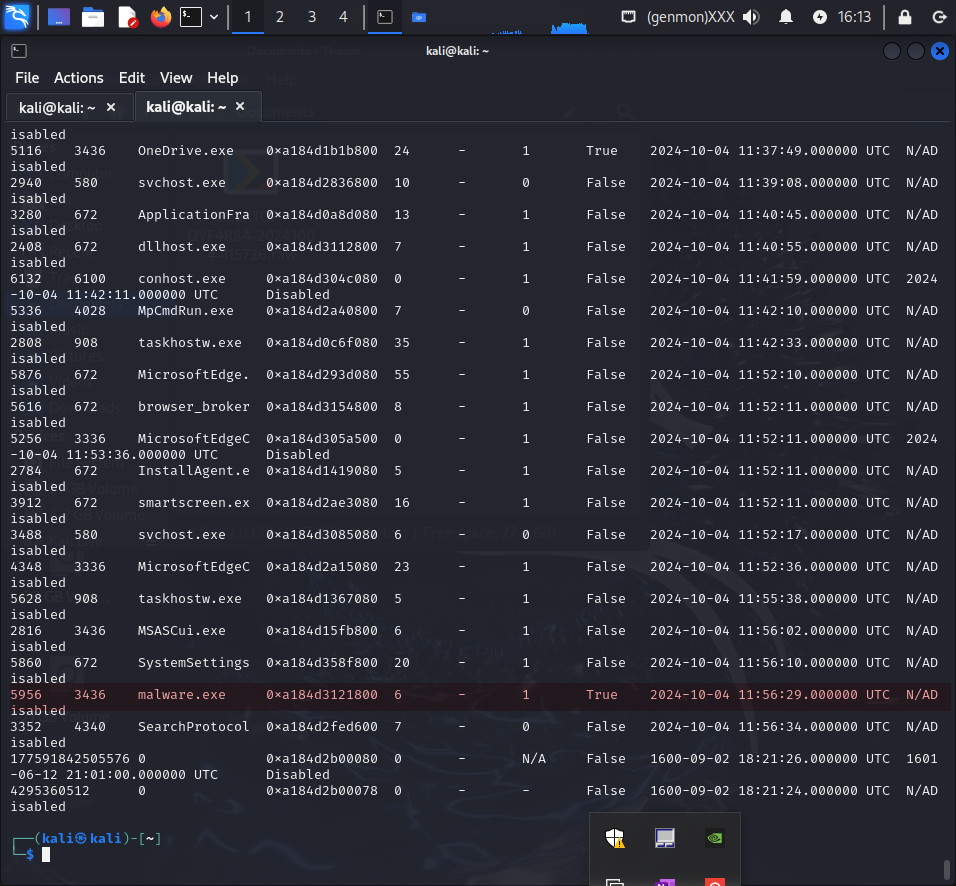
Nous avons effectué l’extraction d’information de la machine Windows de bob avec le logiciel **Dumplt.exe** le 04/10/2024 à 11h57 que vous avons transféré dans notre machine pour analyser dans le répertoire **/home/kali/Documents/**



L’analyse du fichier **DESKTOP-QVF4R8A-20241004-115726.raw** l’outil **volatility** à 3h07avec la commande volatility **python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.info.Info** qui a permis d’avoir quelque information sur notre copie de la RAM

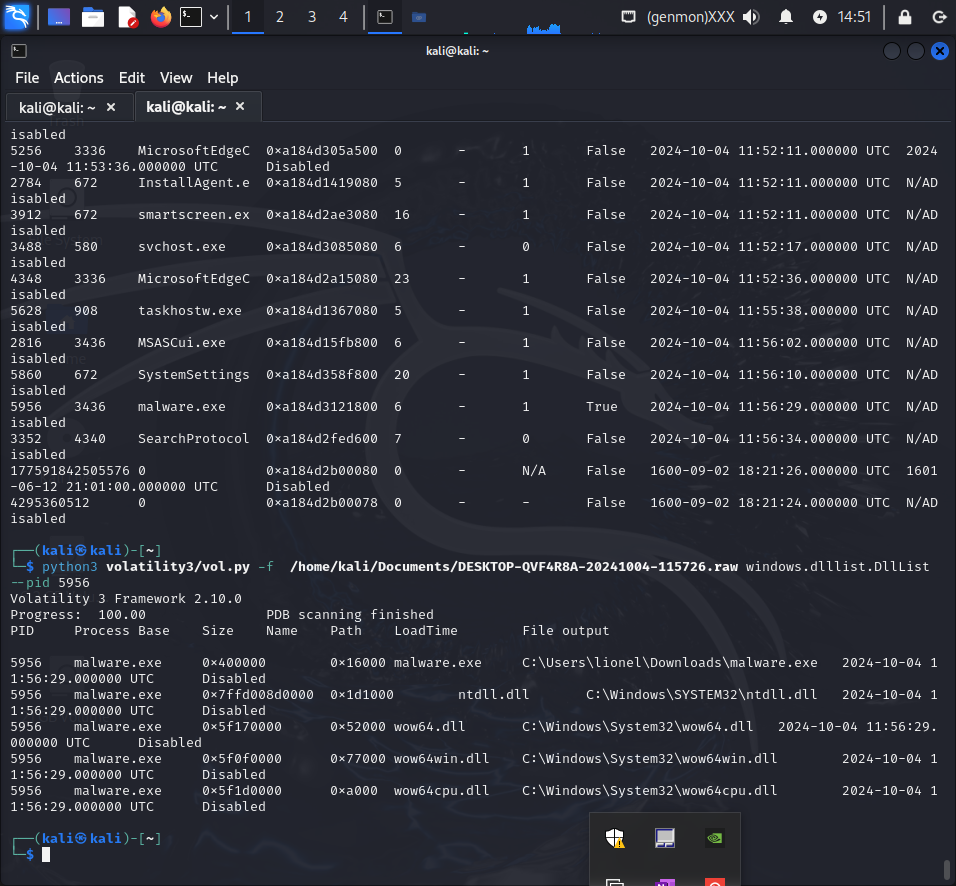


La commande **python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.pslist.PsList** va lister tous les processus en cours à fin de voir s’il y à pas une processus malveillant qui exécutait au moment du dump



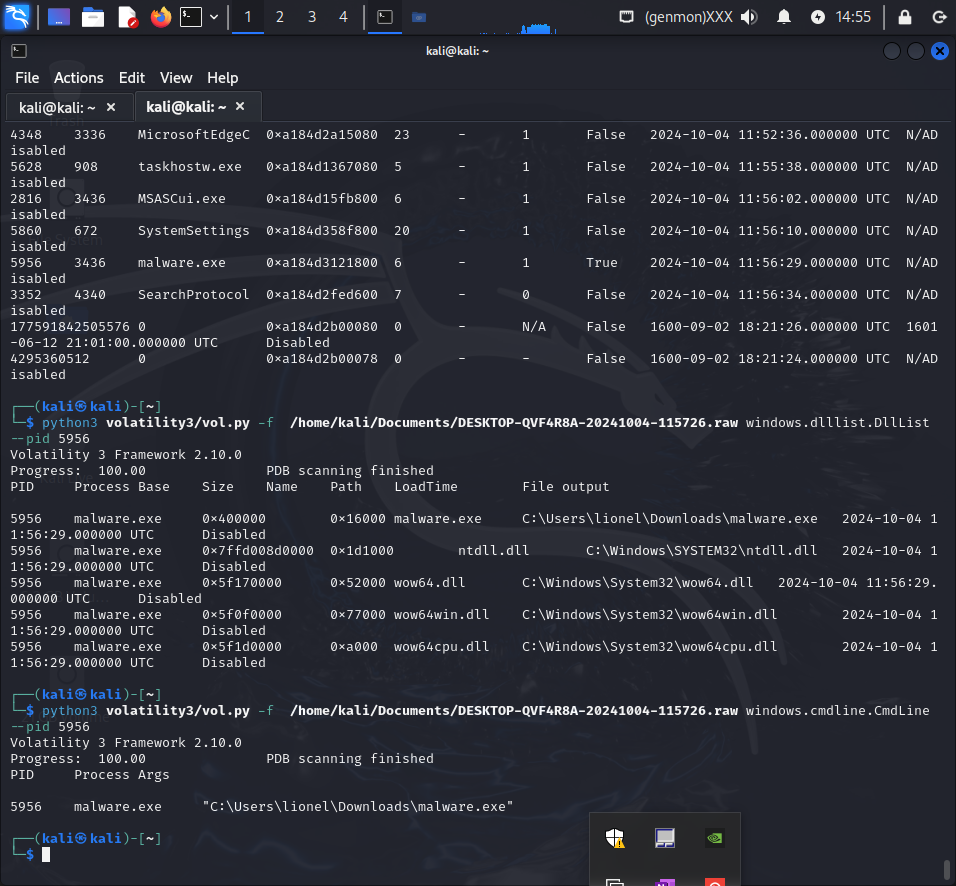
Après cette analyse on soupçonne que le fichier **malware.exe** en cours d’exécution dans les processus est fichier malveillant.

Pour vérifier nos dire on a utiliser la **commande python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.dlllist.DllList --pid 5956**



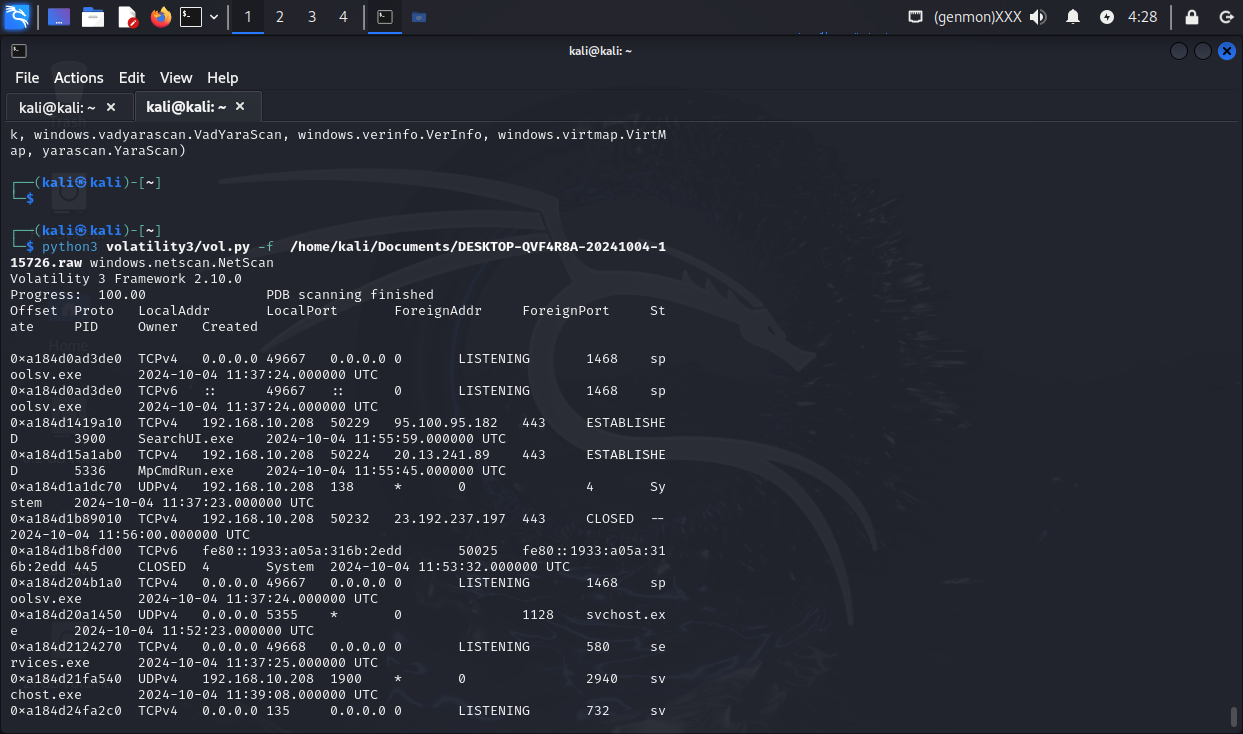
Nous remarquons la présence du même fichier d’où potentiellement une activité malveillante.

Vérifions maintenant si le logiciel malveillant à lancer des programmes avec la commande **python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.cmdline.CmdLine --pid 5956**



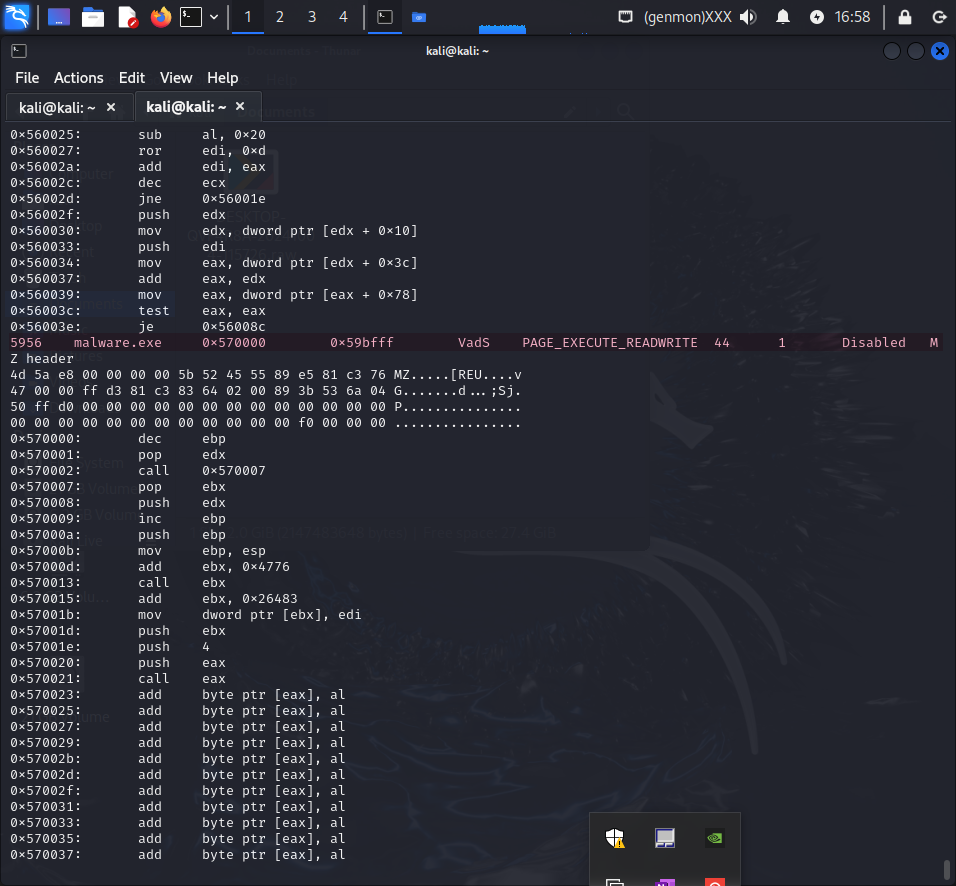
Nous remarquons une activité au niveau du répertoire utilisateur.

Par la suite nous allons vérifier s’il y a une connexion établie, avec la commande **python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.netscan.NetScan**

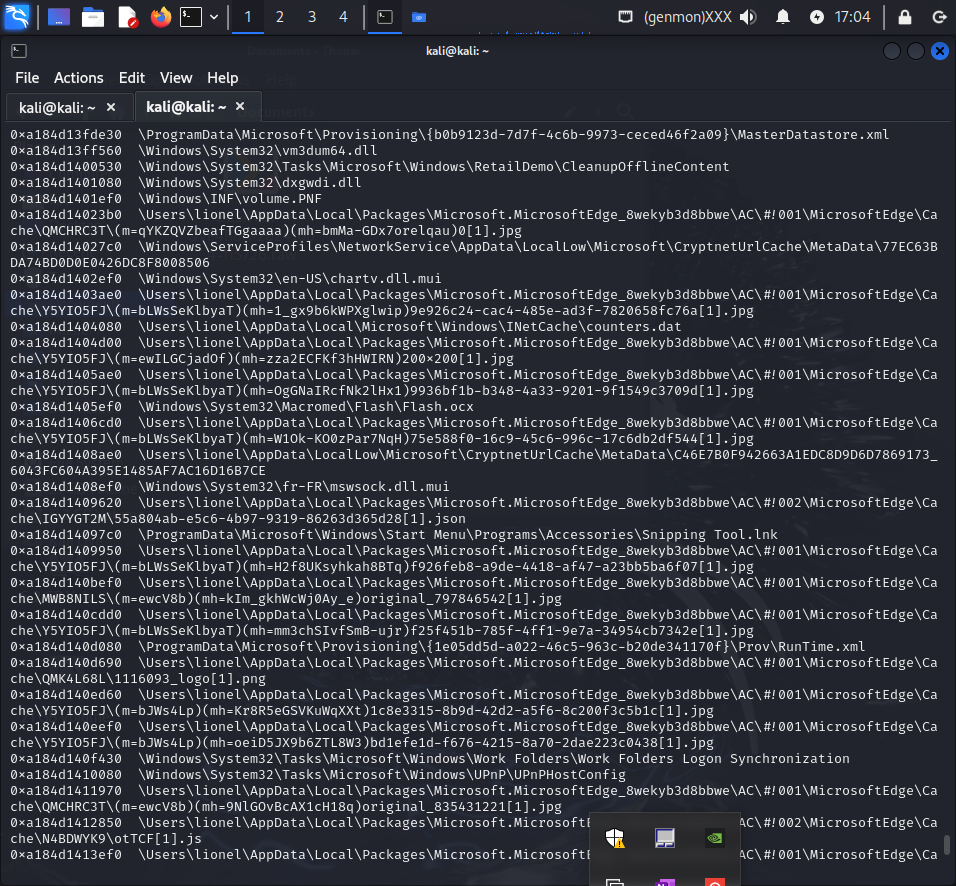


La commande

**python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.malfind.Malfind** va permettant d’analyser les fichiers qui était exécuter au moment dump de la mémoire vive



La commande **python3 volatility3/vol.py -f /home/kali/Documents/DESKTOP-QVF4R8A-20241004-115726.raw windows.filescan.FileScan** pour permettre d’analyser les fichier cachées



**Les résultats trouvés et la conclusion**

- Malware.exe (PID 5956) : Le processus le plus suspect dans cette capture est `malware.exe`, qui se trouve dans le répertoire `C:\Users\lionel\Downloads\malware.exe`. Il est courant pour les malwares d’être placés dans des répertoires de téléchargements, souvent via des téléchargements directs ou par des scripts malveillants. Le fait qu’il soit exécuté sur le système est un indicateur très fort d’une activité malveillante.  
   - La ligne de commande montre son exécution à partir du répertoire utilisateur, ce qui renforce l’hypothèse d'un téléchargement et d'une exécution manuels ou via un exploit.

**SOMMAIRE DES RESULTATS TROUVES**

1. **Fichiers concernés par l’enquête**

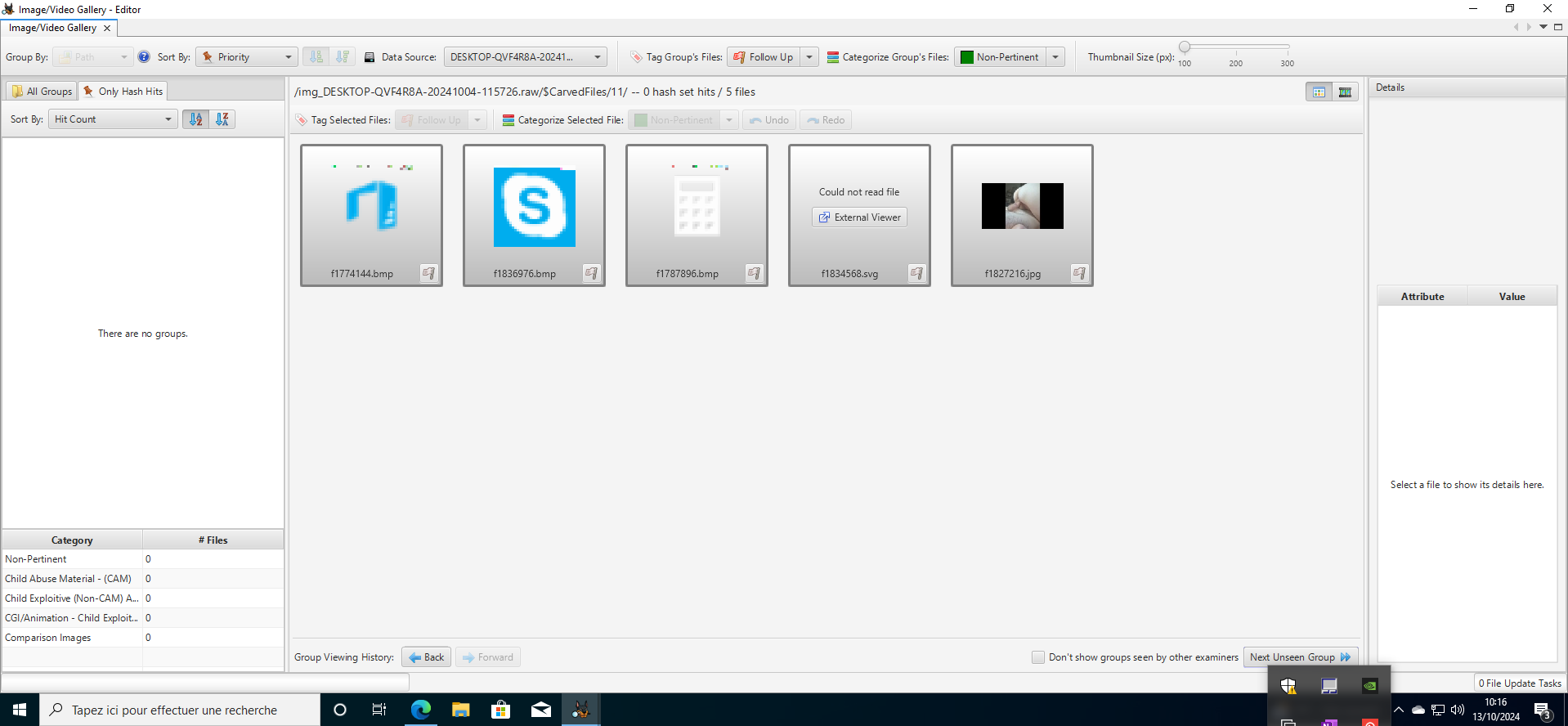
Nous avons identifié un fichier comme pertinent pour l’enquête, notamment un malware qui pourrais d’être utilisé pour accéder à des informations sensibles de l’entreprise.

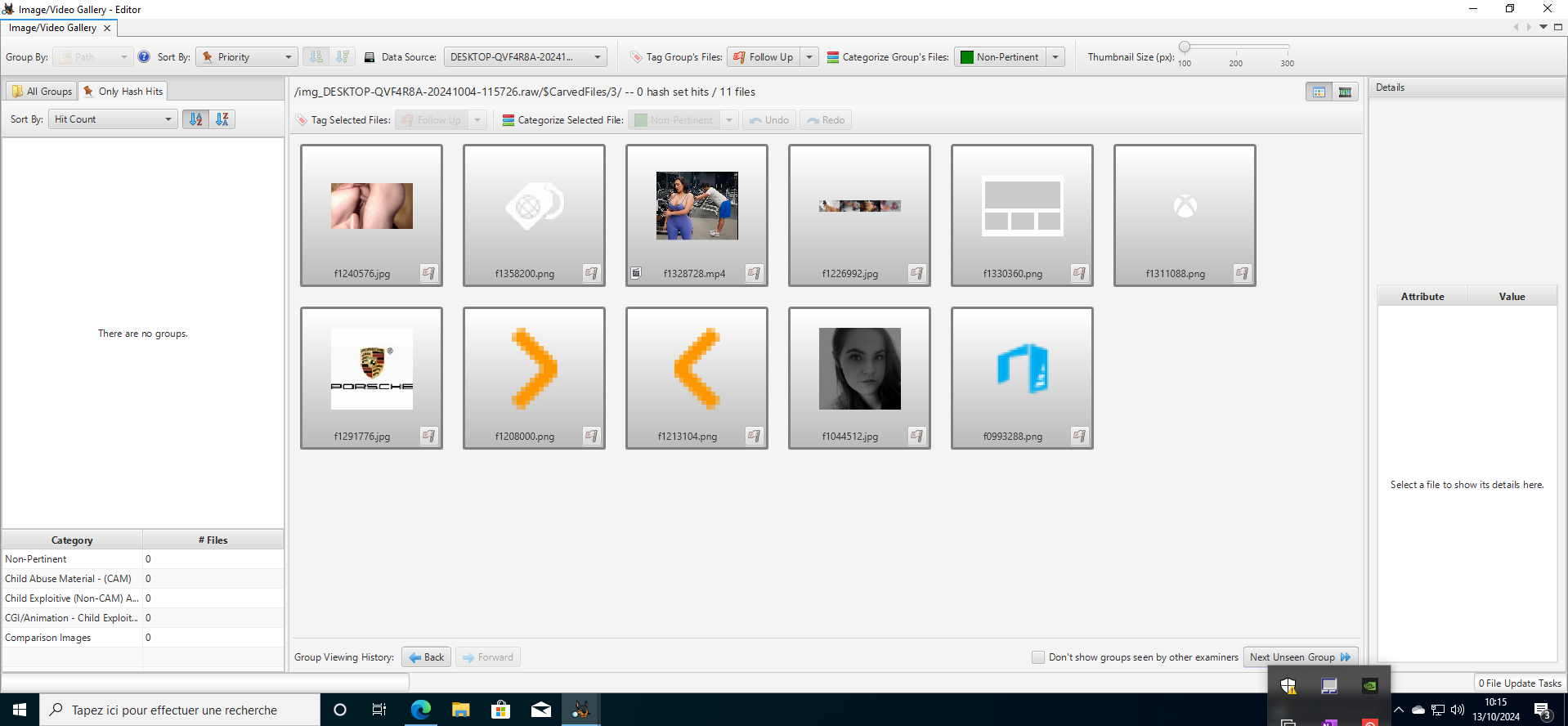
1. **Chaîne de caractères et mots-clés utilisés**

Des chaînes de caractères en lien avec des recherches sur des sites inappropriés ont été trouvées dans la mémoire vive

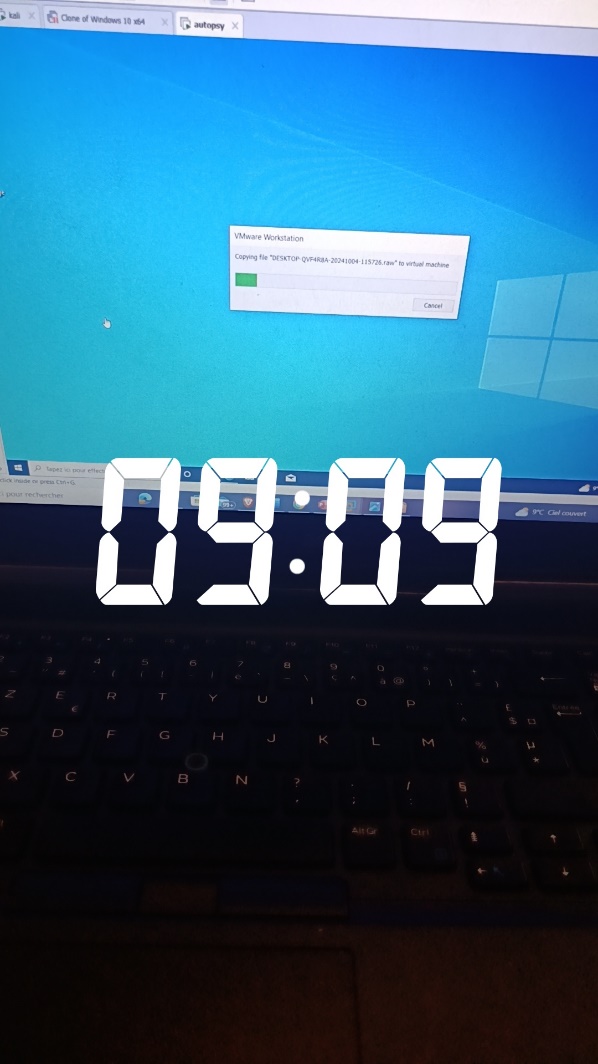
1. **Preuve relative à l’internet**

Des fichiers sensibles et inappropriés ont été récupérés, tels que : les images, et les vidéos





**Documentation de la chaîne de custodie**

Début de l’analyse sur la machine de bob à 9h09 le 12/10/2024

Pause de 1h à 12h30



Reprise de l’enquête à 17h 00

