

# Investigations Numériques

version : 17-02-2017 08:52



Thomas Duval

[thomas.duval@orange.com](mailto:thomas.duval@orange.com)

[Sommaire](#)

## Sommaire

version : 13-11-2014 21:11

[\\$:/tags/SideBar](#)

- [1\) Introduction](#)
- [2\) Know your Enemy](#)
- [3\) Méthodes](#)
- [4\) Techniques](#)
- [5\) Outils](#)
- [6\) Mobile](#)
- [7\) Conclusions](#)

# 1) Introduction

version : 17-02-2017 08:53

[TableOfContents](#)

Sommaire :

- [Vocabulaire](#)
- [Qui fait quoi ?](#)

## 1.1) Vocabulaire

version : 17-02-2017 08:53

### Définition

#### **incident de sécurité selon ISO27035**

un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information.



### Forensics

- Computer Forensics
  - Network forensics
  - Social forensics
  - ...
- Analyses numériques
- **Investigations numériques**
- Inforensique
- Analyse forensique

[Termes génériques](#)

[Critères de sécurité](#)

[Définition d'une menace](#)

# Termes génériques

version : 06-10-2014 07:57

## **hacker :**

ou bidouilleur informatique, une personne qui montre une passion pour la compréhension du fonctionnement intime des systèmes, ordinateurs et réseaux informatique

## **pirate informatique :**

personne qui utilise les ordinateurs ou les réseaux informatiques pour effectuer des actions (délits ou crimes) malveillantes et punies par la loi.

## **black / grey / white hat :**

dénomination permettant de délimiter les objectifs et la légalité des actes des hackers / pirates

# Critères de sécurité

version : 29-11-2015 21:11

## **l'intégrité :**

Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

## **la confidentialité :**

Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

## **la disponibilité :**

Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

## **la non-réputation et l'imputation :**

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

## **l'identification, l'authentification, l'autorisation :**

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

# Définition d'une menace

version : 25-11-2014 11:43

Une menace peut être

- Interne au réseau de l'entreprise
- Externe, c'est-à-dire sur Internet (en général)



Une menace peut provenir :

- un utilisateur autorisé du système
- une personne malveillante
  - Qui ne peut pas s'authentifier sur le système
  - Qui a pu s'authentifier sur le système
- un programme malveillant
  - Déposé par mail
  - Déposé sur une clé USB anodine
- un sinistre
- une erreur humaine
- ...

## 1.2) Qui fait quoi ?

version : 17-02-2017 09:03

# La police

## L'OCLCTIC



*Office Central de Lutte contre la Criminalité liée aux Technologies de*

## *I'Information et de la Communication*

Source : [police-nationale.interieur.gouv.fr](http://police-nationale.interieur.gouv.fr)

- **animer et coordonner** la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication ;
- **procéder**, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigations ;
- apporter, à leur demande, une **assistance** aux services de police, de gendarmerie et de douane en cas d'infractions liées aux hautes technologies ;
- **intervenir**, avec l'accord de l'autorité judiciaire saisie, pour s'informer sur place des faits relatifs aux investigations conduites ;
- **centraliser et diffuser** l'information sur les infractions technologiques à l'ensemble des services répressifs.

## BEFTI

*Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information*

Source : [www.prefecturedepolice.interieur.gouv.fr](http://www.prefecturedepolice.interieur.gouv.fr)

Crée en février 1994, la BEFTI compte aujourd'hui 25 policiers spécialisés dans les nouvelles technologies. Elle est composée de trois groupes « enquêtes et initiative » et d'un groupe d'« assistance ».

Les investigations des groupes d'enquêtes portent sur les crimes et délits informatiques :

- intrusion dans un ordinateur ou un réseau ;
- contrefaçon de logiciels ou de bases de données ;
- téléchargements illégaux ;
- piratage de réseau téléphonique ;
- défiguration de sites sensibles ;
- modification ou suppression de données ;
- défaut de sécurisation des données personnelles,
- collectes frauduleuses, illicites ou déloyales de données à caractère personnel.

## La gendarmerie

Institut de recherche criminelle (IRCGN) situé dans l'enceinte du Service technique de recherches judiciaires et de documentation (STRJD) au Fort de Rosny-sous-Bois (Seine-Saint-Denis).

- « **activités criminalistiques** »
  - extraction de données,
  - analyse de traces numériques,
  - études des réseaux télécoms et des virus
- « **activités transverses** »
  - guichet unique téléphonie et Internet pour contacter plus rapidement les bons interlocuteurs chez les opérateurs,
  - R&D,
  - outils communautaires
- « **activités judiciaires** »
  - atteintes aux mineurs sur Internet,
  - analyse des images de pédopornographie et
  - investigations sur Internet.

## L'entreprise

### OSSI

#### **Officier de Sécurité des Systèmes d'Information**

L'officier de sécurité est l'officier qui a pour mission, sous les ordres de son autorité d'emploi, de fixer les règles et consignes de sécurité à mettre en oeuvre relatives aux personnes et aux informations ou supports protégés et d'en vérifier l'exécution.

### DSI

#### **Direction des Systèmes d'Information**

Le DSI d'une organisation (entreprise, association, etc.) est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels du système d'information, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre.

## L'expert judiciaire

Un expert judiciaire ou témoin expert est une personne morale ou une personne physique qualifiée dans un domaine autre que le droit. L'expert judiciaire assiste une cours de justice pour des expertises bien précises. L'expert judiciaire prête serment une fois pour toute avant sa première mission s'il est inscrit sur une liste de cour d'appel ou une liste nationale. S'il n'est pas choisi parmi une liste, il devra obligatoirement prêter serment avant sa mission et un PV sera joint au dossier. Le serment prêté en Cour d'appel par l'expert judiciaire est le suivant :

« Je jure, d'apporter mon concours à la Justice, d'accomplir ma mission, de faire mon rapport, et de donner mon avis en mon honneur et en ma conscience. »

Il doit suivre les règles de déontologie : [http://www.cncej.org/documents/uploads/246\\_REGLES\\_DEONTOL\\_090512.pdf](http://www.cncej.org/documents/uploads/246_REGLES_DEONTOL_090512.pdf)

## PNIJ

Plateforme Nationale des Interceptions Judiciaires Situé dans un campus de Thales à Elancourt, dans les Yvelines, à l'abri théorique d'un crash d'avion.

Cette plateforme permet d'intercepter des communications téléphoniques de manière plus "professionnelle"...

Ce système d'interception, d'écoute, d'identification, de géolocalisation, de stockage des échanges téléphoniques ou électroniques permettra de traiter en un lieu unique (...) la masse annuelle des 5 millions de réquisitions judiciaires et 40 000 écoutes autorisées par les juges.

via <http://questions.assemblee-nationale.fr/q14/14-28378QE.htm>

<http://cybercriminalite.wordpress.com/2014/10/29/le-decret-portant-creation-de-la-plate-forme-nationale-des-interceptions-judiciaires-pnij-a-ete-publie-le-9-octobre/>

## CECyF

<http://www.cecylf.fr/>

Le Centre Expert contre la Cybercriminalité Français est une association permettant aux services chargés de l'application de la

loi, aux chercheurs de toutes origines (académiques, industriels, indépendants) et aux établissements d'enseignement de se rencontrer et d'échanger pour créer des projets qui contribuent à la formation, l'éducation et la recherche contre la cybercriminalité.

## C3N

C'est le centre de lutte contre les criminalités numériques.

L'objectif est de patrouiller sur Internet à la recherche d'infraction, un peu comme la BAC dans la vie réelle. Ces gendarmes utilisent un certain nombre d'outils qui leur permettent d'effectuer des recherches sur Twitter, sur le "deep" web et dans les jeux en ligne (Clash of Clan, Call of Duty, ...)

via <http://www.industrie-techno.com/cybercriminalite-la-boite-a-outils-des-gendarmes-du-net.42006?platform=hootsuite>

## Point de vue mondial

### CERT (Computer Emergency Response Team)

Ce sont les centres gouvernementaux de veille, d'alerte et de réponse aux attaques informatiques.

Par exemple pour la France le CERT-FR (anciennement CERTA) :  
<http://www.cert.ssi.gouv.fr/>

Ses principales missions peuvent se décliner ainsi :

- détecter les vulnérabilités des systèmes, au travers notamment d'une veille technologique ;
- piloter la résolution des incidents, si besoin avec le réseau mondial des CERT ;
- aider à la mise en place de moyens permettant de se prémunir contre de futurs incidents ;
- organiser la mise en place d'un réseau de confiance.

Le CERT-FR est membre du FIRST depuis le 12 septembre 2000 et participe à l'activité de la TF-CSIRT (Computer Security Incident Response Team) qui est la coordination des CERT européens (Trusted Introducer Level 2 ou niveau Accredited depuis le 25 mars 2002).

# FIRST

Il permet de fédérer l'ensemble des équipes de réaction aux incidents concernant la sécurité des systèmes d'information (<http://www.first.org>). Les buts du FIRST sont les suivants :

- favoriser la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d'incident de sécurité informatique ;
- fournir un moyen de communication commun pour la diffusion de bulletins et d'alertes sur des failles potentielles et les incidents en cours ;
- aider au développement des activités de ses membres, en particulier, la recherche et les activités opérationnelles ;
- faciliter le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques.

## 2) Know your Enemy

version : 26-09-2014 21:28

TableOfContents

Sommaire :

- Taxonomie
- Analyse d'une attaque
- Pirates célèbres
- Les dernières attaques
- Quelques articles de loi

### 2.1) Taxonomie

version : 29-11-2015 21:44

Taxonomie par l'ANSSI <http://www.ssi.gouv.fr/archive/fr/documentation/650/> :

- Agresseurs
- Fraudeurs
- Employés malveillants
- Militants
- Espions
- Terroristes

Autres taxonomie :

- Cyber criminals
- Spammers and adware spreaders
- Advanced persistent threat (APT) agents
- Corporate spies
- Cyber warriors
- Hactivists
- Rogue hackers

## Agresseurs

version : 06-10-2014 08:04

### **hacker ou passionné**

individu **curieux**, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il **ne nuit pas intentionnellement** et possède souvent un code d'honneur et de conduite. En général il n'a pas conscience de la mesure de ses actes. L'agresseur passionné est de moins en moins expérimenté.

### **cracker ou casseur**

plus **dangereux** que le hacker, **cherche à nuire** et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

## Fraudeurs

version : 06-10-2014 08:04

Le fraudeur bénéficiant souvent d'une **complicité**, volontaire ou non, chez ses victimes, il cherche à **gagner de l'argent** par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme organisé ou non, il peut :

- attaquer une banque,
- falsifier des cartes de crédit ou
- se placer sur des réseaux de transferts de fonds et,
- si c'est un particulier, il peut vouloir falsifier sa facture d'électricité ou de téléphone.

# Employés malveillants

version : 06-10-2014 08:05

## Le fraudeur interne

possède de **bonnes compétences** sur le plan technique, il est souvent informaticien et sans antécédents judiciaires. Il peut penser que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur.

Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Il peut répondre à un besoin matériel personnel qui induit des conduites de dépendances (jeux, sexe...). Pour parvenir à ses fins, il **possède les moyens**, qu'il connaît parfaitement, et qui ont été mis à sa disposition par son entreprise.

# Militants

version : 06-10-2014 08:05

**Motivés par une idéologie ou la religion**, ils disposent de compétences techniques très variables. Leurs objectifs peuvent être limités à la diffusion massive de messages, comme ils peuvent s'étendre à des nuisances effectives sur les systèmes d'information des organismes en opposition avec leur idéologie.

# Espions

version : 06-10-2014 08:05

Ils participent à la guerre économique. Ils travaillent pour un État ou pour un concurrent. Ils sont **patients** et **motivés**. Ils savent garder le secret de leur réussite pour ne pas éveiller les soupçons et continuer leur travail dans l'ombre. Ils agissent souvent depuis l'intérieur de l'organisme, \* soit en ayant trouvé un moyen d'y pénétrer, \* soit en soudoyant une personne ayant accès aux biens. Ils ont pour but de **voler des informations** ou de **détruire des données stratégiques** (vitales) pour l'organisme. Dans tous les cas, les espions ont un excellent niveau de maîtrise de soi, ainsi qu'une grande capacité d'adaptation aux environnements.

# Terroristes

version : 06-10-2014 08:06

Souvent appelés les **cyber-terroristes**, moins courants, les terroristes sont aidés dans leur tâche par l'interconnexion et l'ouverture croissante des réseaux : **très motivés**, ils veulent faire peur et faire parler d'eux. Les actions se veulent **spectaculaires, influentes, destructrices, meurtrières**. Ce profil est pris de plus en plus au sérieux par les États depuis l'attentat du 11 septembre 2001. Ils considèrent qu'une cyber-attaque perpétrée par un terroriste pourrait gravement nuire aux infrastructures économiques et critiques d'un État devenu très dépendant de ses systèmes d'informations vitaux.

# Cyber criminals

version : 25-02-2015 21:12

Ce sont des pirates professionnels Leur but est de voler de l'argent en :

- Manipulant les comptes bancaires
- Volant les numéros bancaires
- Volant des logins / password
- ...

# Spammers and adware spreaders

version : 25-02-2015 21:13

## aggressive marketer

Ce sont des pourvoyeurs de spams et de pub Ils travaillent à leur compte ou pour des entreprises légitimes

# Advanced persistent threat (APT)

## agents

version : 25-02-2015 21:13

Ils appartiennent à des groupes bien financés et très organisés

Ils pénètrent discrètement les réseaux des sociétés pour voler des informations confidentielles

Ils sont généralement localisés dans des pays voisins de leurs victimes

Ils visent les gains à long terme

## Corporate spies

version : 25-02-2015 21:13

Ils appartiennent à des groupes bien financés et très organisés

Ils pénètrent discrètement les réseaux des sociétés pour voler des informations confidentielles

Ils sont généralement localisés près de leurs victimes

Ils visent les gains à court ou moyen terme

## Cyber warriors

version : 25-02-2015 21:13

Leurs attaques sont motivées par

- la religion,
- la politique,
- l'environnement,
- etc.

Ils utilisent en général le « web defacement »

Contre-exemple : Wikileaks

## Hactivists

version : 28-11-2018 09:17

Leur objectif prioritaire est la désactivation des capacités militaires d'un adversaire

Les attaquants peuvent être des « APT agent » ou des « corporate spies »

Le ver Stuxnet en est un bon exemple

## Rogue hackers

version : 28-11-2018 09:17

Le reste des pirates

Ils ne veulent que prouver leurs capacités, vanter leurs capacités, ...

Ils ne font pas (en général) de gros dégâts

## 2.2) Analyse d'une attaque

version : 29-11-2015 21:54



**Comment attaque t'on un système informatique ?**

Hide

*Les actions listées ci-dessous ne sont pas exhaustives et ne sont pas systématiques.*

## Recherche et analyse

L'attaquant va commencer par rechercher et analyser sa cible. Il va effectuer les actions suivantes :

- Recherche sur Internet (Google, Yahoo, DNS, ...)
- Recherche sur les réseaux sociaux
- Recherche d'un ou de plusieurs points d'entrée
- Scan des machines ciblées
- Analyse des réponses reçues

## Intrusion

- Développement ou récupération d'un logiciel d'attaque
- Mise en place d'une chaîne de proxy pour ne pas s'exposer
- Exécution de l'intrusion

## Maintien de connexion

- Obtention d'un compte d'administration / élévation de privilèges
- Suppression de pirate qui auraient déjà accès à la machine
- Mise en place d'un patch / Colmatage de la vulnérabilité utilisée

## Camouflage

Pour éviter d'être détecter par un administrateur, l'attaquant va camoufler ses actions et ses connexions :

- création d'un compte d'administration anodin
- utilisation d'un rootkit

## Exploitation

Une fois le pirate bien installé, il peut commencer à "travailler" et il peut utiliser la machine :

- comme rebond vers le réseau interne de l'entreprise
- comme rebond vers des serveurs externes :
  - pour effectuer des dénis de service distribués (DDOS)
  - pour l'utiliser comme proxy pour cacher ses connexions
  - pour l'utiliser comme un serveur de CC (Command & Control)
  - ...
- comme serveur pour faire du "bitcoins mining"
- ...

## 2.3) Pirates célèbres

version : 06-10-2014 08:15

### **Kevin Mitnick**

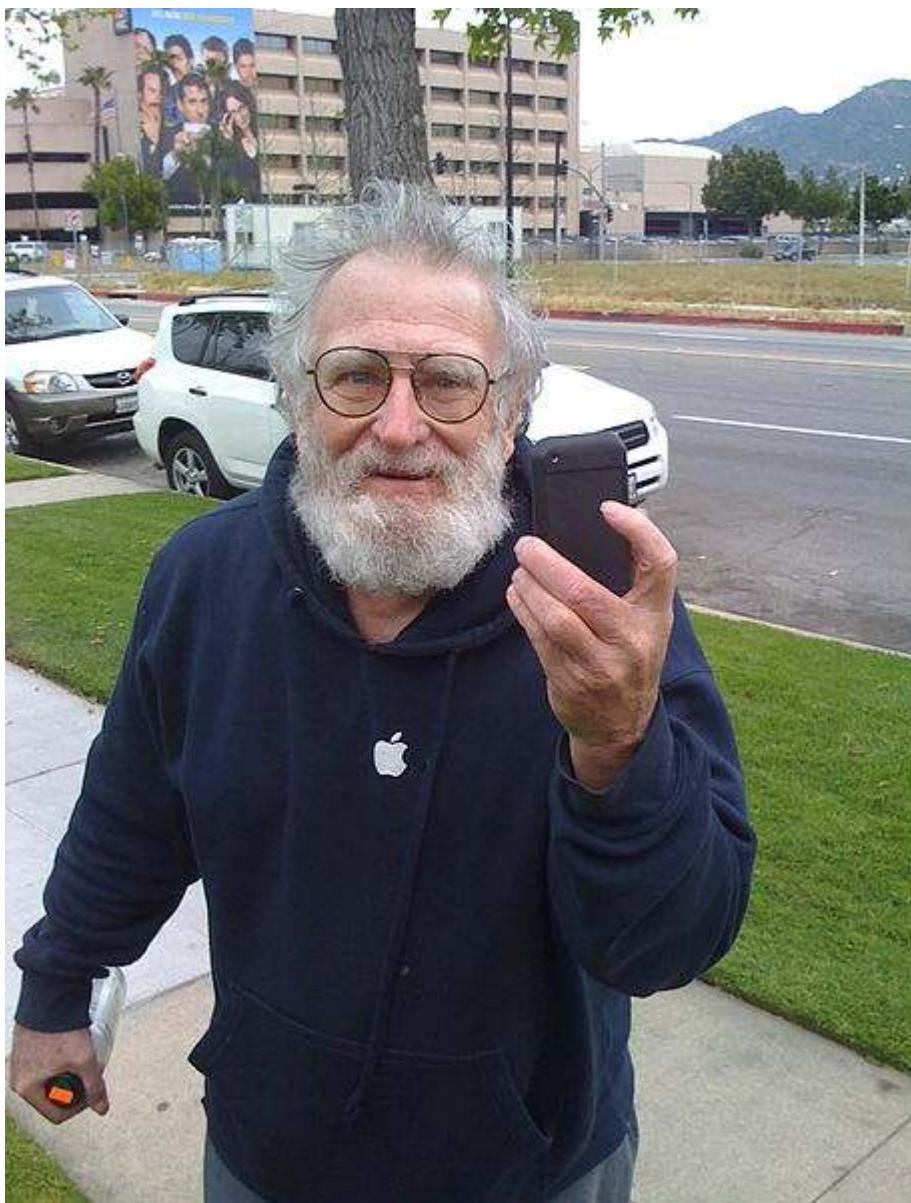
il s'est infiltré dans certains des plus grands sites internet sécurisés,

comme celui du Pentagone.  
il est connu notamment de par son *combat* avec Tsutomu Shimomura



**John Draper alias *Captain Crunch***

Célèbre phreaker américain



**H.D Moore**

Créateur du framework Metasploit

**Gary McKinnon alias Solo**

accusé d'avoir pénétré dans 97 ordinateurs appartenant à l'US Army et à la NASA.

**LulSec**

Composé d'un noyau de 6 personnes, dont certaines issues du collectif Anonymous, ses membres ont tous été arrêtés dans l'année suivant son activité.





## Anonymous

Mouvement *hacktiviste*, se manifestant notamment sur Internet

Chris Lander, Baltimore City Paper (2 avril 2008)

« Anonymous est la première superconscience construite à l'aide de l'Internet.

Anonymous est un groupe semblable à une volée d'oiseaux.

Comment savez-vous que c'est un groupe ?

Parce qu'ils voyagent dans la même direction.

À tout moment, des oiseaux peuvent rejoindre ou quitter le groupe,  
ou aller dans une direction totalement contraire à ce dernier »



## 2.4) Les dernières attaques

version : 29-11-2015 21:58

[cf. formation entreprise](#)

## 2.5) Quelques articles de loi

version : 06-10-2014 08:24

<http://www.securiteinfo.com/legal/synthesepeines.shtml>

# Code pénal relatifs au piratage informatique

### Articles 323-1

Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002

- Le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende.

### Article 323-2

Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002

- Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

## 3) Méthodes

version : 26-09-2014 21:28

[TableOfContents](#)

Sommaire :

- Objectifs de la réponse aux incidents
- Difficultés
- Inventaire
- Répondre à un incident

- Exemples de réponse à un incident

## 3.1) Objectifs de la réponse aux incidents

version : 26-01-2015 21:12

- Déetecter les incidents de sécurité
- Minimiser les pertes et les destructions
- Atténuer les faiblesses exploitées
- **Rétablir les services le plus rapidement**

## 3.2) Difficultés

version : 12-10-2014 17:36

Dépend d'un grand nombre de disciplines

En perpétuel mouvement

Les attaquants ont souvent une longueur d'avance :

- en terme d'attaque
- en terme d'anti-forensics

Les infrastructures sont en perpétuel mouvement :

- de nouveaux produits sortent chaque jour
- de nouvelles infrastructures aussi (cloud, ...)

La discipline reste basée sur l'expérience des enquêteurs.

## 3.3) Inventaire

version : 06-10-2014 08:25

Pour aller sur le lieu d'un délit informatique et pour pouvoir récupérer des preuves, il faut ceci (tiré du [Blog de Zythom](#)) :

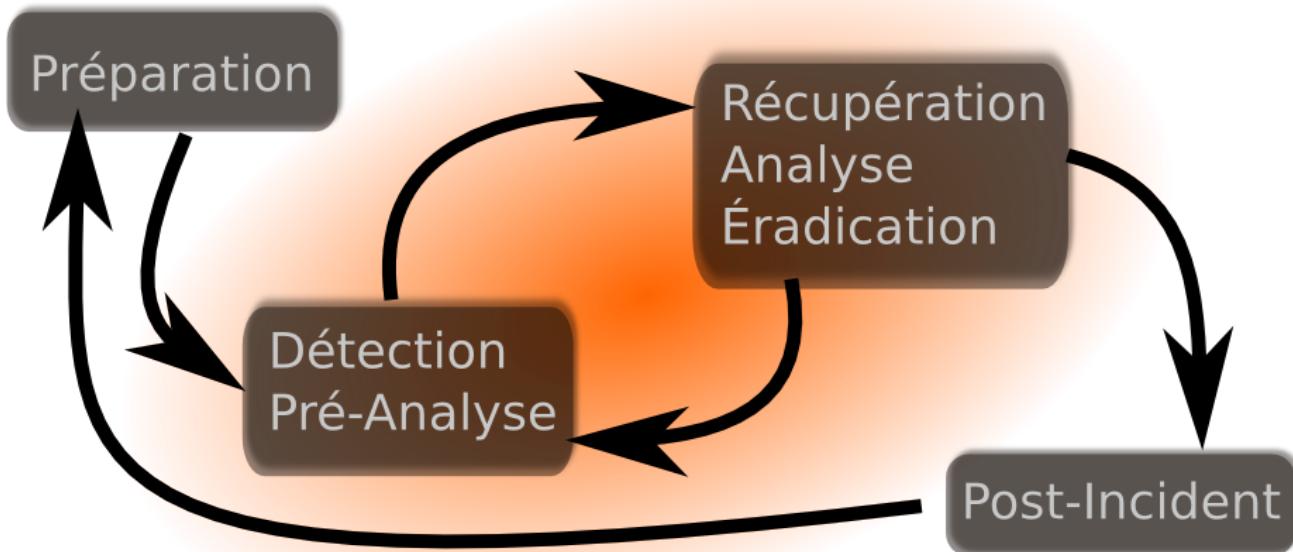
- le boot CD d'analyse inforensique DEFT
- les outils de l'informaticien (tournevis de toutes tailles et de toutes

formes)

- stylos et bloc notes (rien de plus gênant que d'avoir à demander sur place)
- un dictaphone numérique
- un ordinateur portable avec carte réseau gigabit et disque de grosse capacité pour la prise d'image en direct (exemple disque dur SATA d'3 To dans un boîtier externe ~USB3)
- une lampe électrique, un bouchon 50 ohms et un connecteur en T ()
- quelques uns des outils conseillés par les dieux des réseaux universitaires
- le live CD d'ophcrack, c'est toujours impressionnant de trouver les mots de passe tout seul
- un câble réseau, un prolongateur et un câble croisé
- une boîte de DVD à graver (et quelques disquettes formatées, cela sert encore...)
- une bouteille d'eau et un paquet de biscuits
- un appareil photo
- un GPS
- du ruban adhésif toile et résistant
- des élastiques de toutes tailles et des trombones.
- un clavier souple ne craignant pas l'humidité avec la connectique qui va bien.
- un tabouret en toile
- vis, patafix, colliers...
- un ventilateur pour les disques
- une petite imprimante
- toute la connectique pour les organisateurs (Palms, Blackberry, iphone, etc.)
- des étiquettes / pastilles de couleur, des stylos et des feutres.
- un petit switch 10/100/1000
- un câble série
- un câble usb
- une nappe IDE
- une nappe SATA
- des adaptateurs USB, SATA, IDE

## 3.4) Répondre à un incident

version : 06-10-2014 08:27



- Préparation
- Détection et Pré-Analyse
- Récupération, Analyse et Éradication
- Post-Incident

## Préparation

version : 06-10-2014 08:27

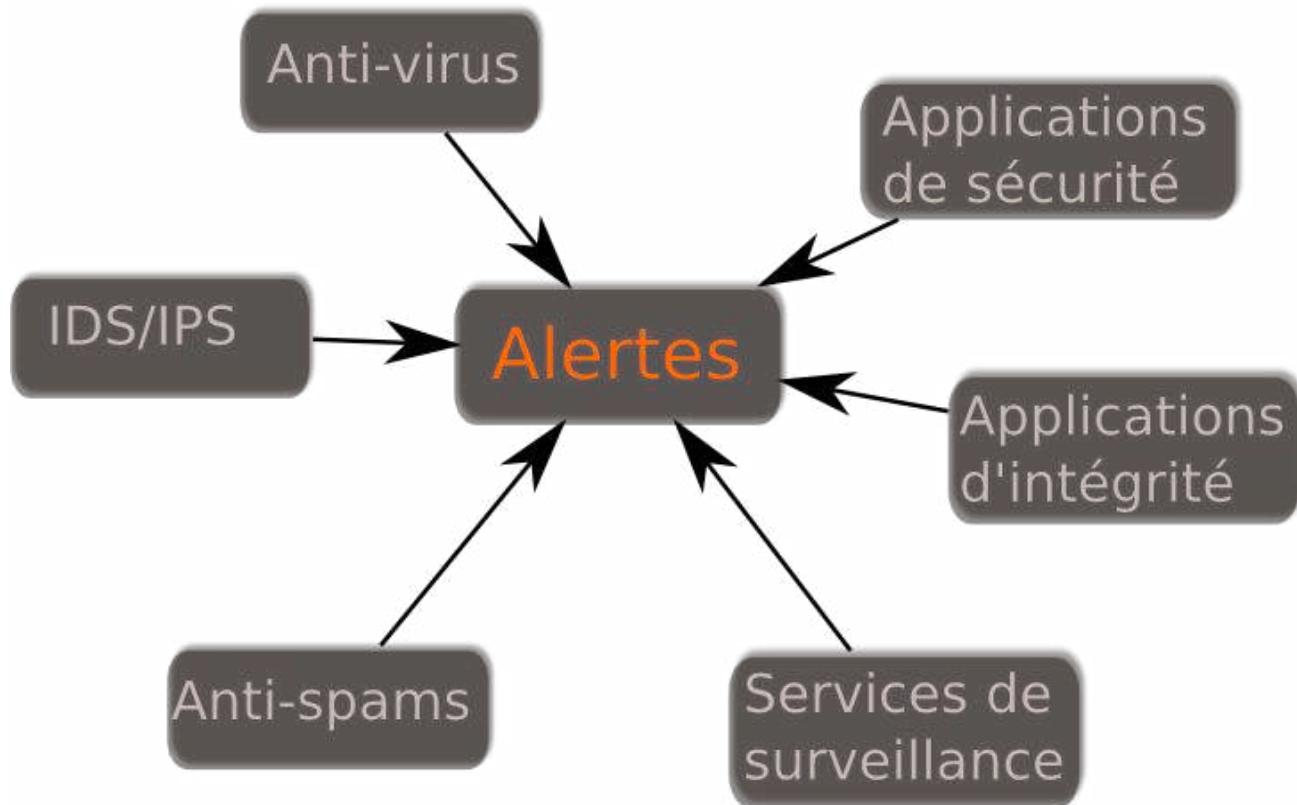
- Formaliser la réponse aux incidents
- Créer une politique de réponse
- Préparer un dispositif de réponse
- Développer des procédures
  - et les faire appliquer dans l'entreprise
  - il faut notamment s'assurer que les techniciens/ingénieurs ne supprimeront pas de données...
- Établir les politiques et les procédures pour le partage d'information
- Préparer les informations à envoyer aux CERT
- Préparer un modèle d'équipe adéquate
- Sélectionner les membres de l'équipe
- Déterminer les services offerts

## Détection et Pré-Analyse

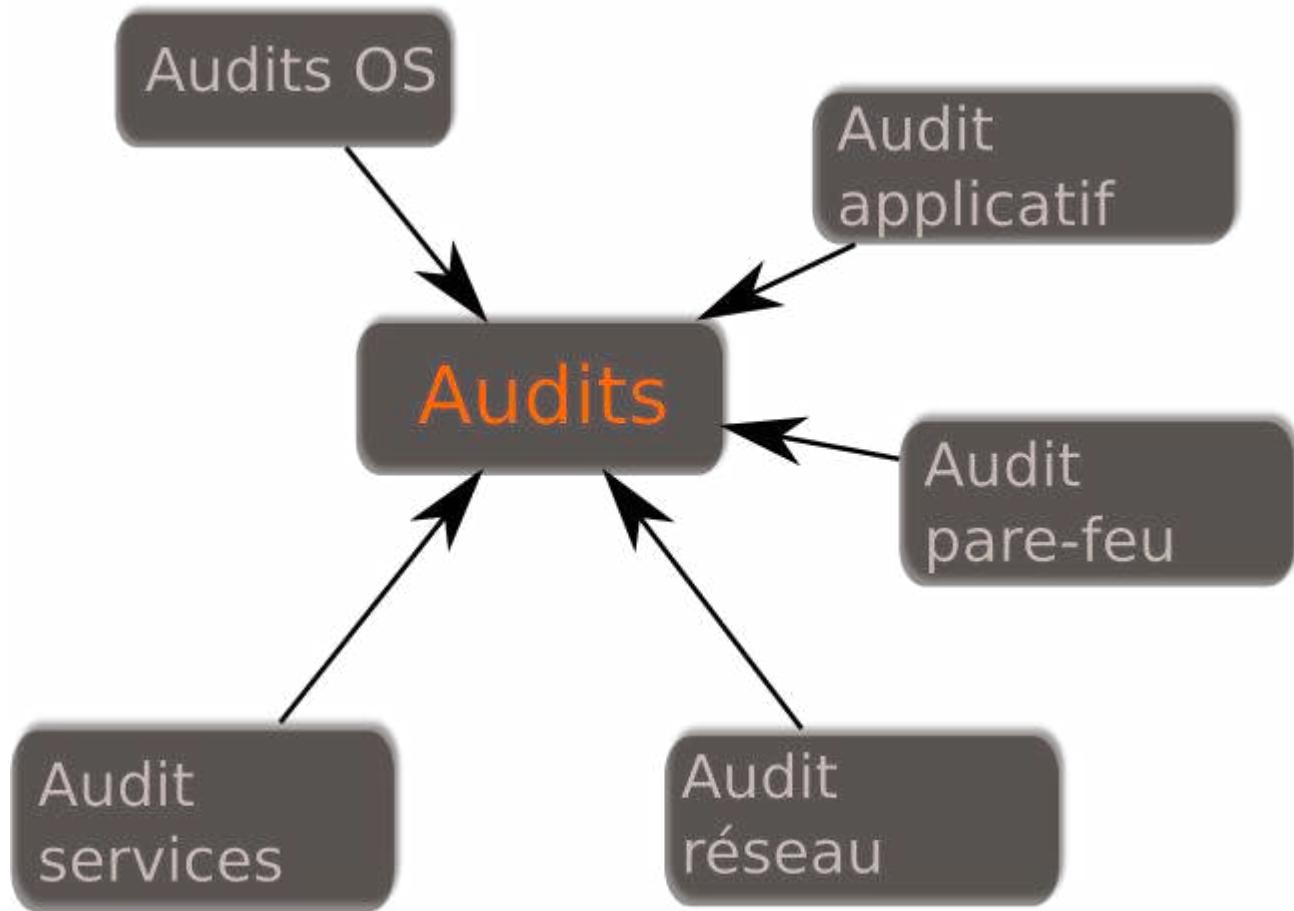
version : 12-10-2014 17:37

# Détection

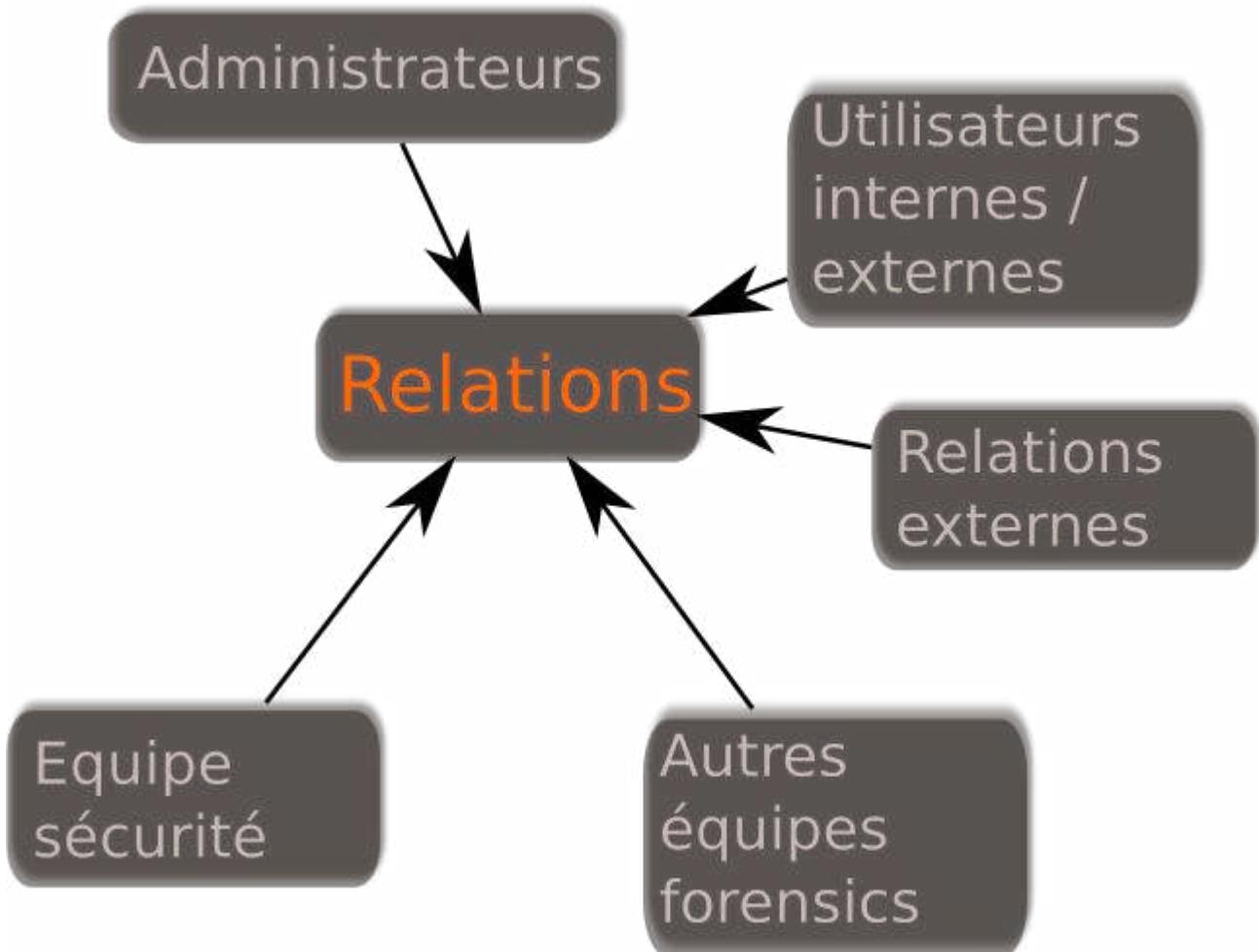
## Alertes



## Audits



## Relations



## Pré-Analyse

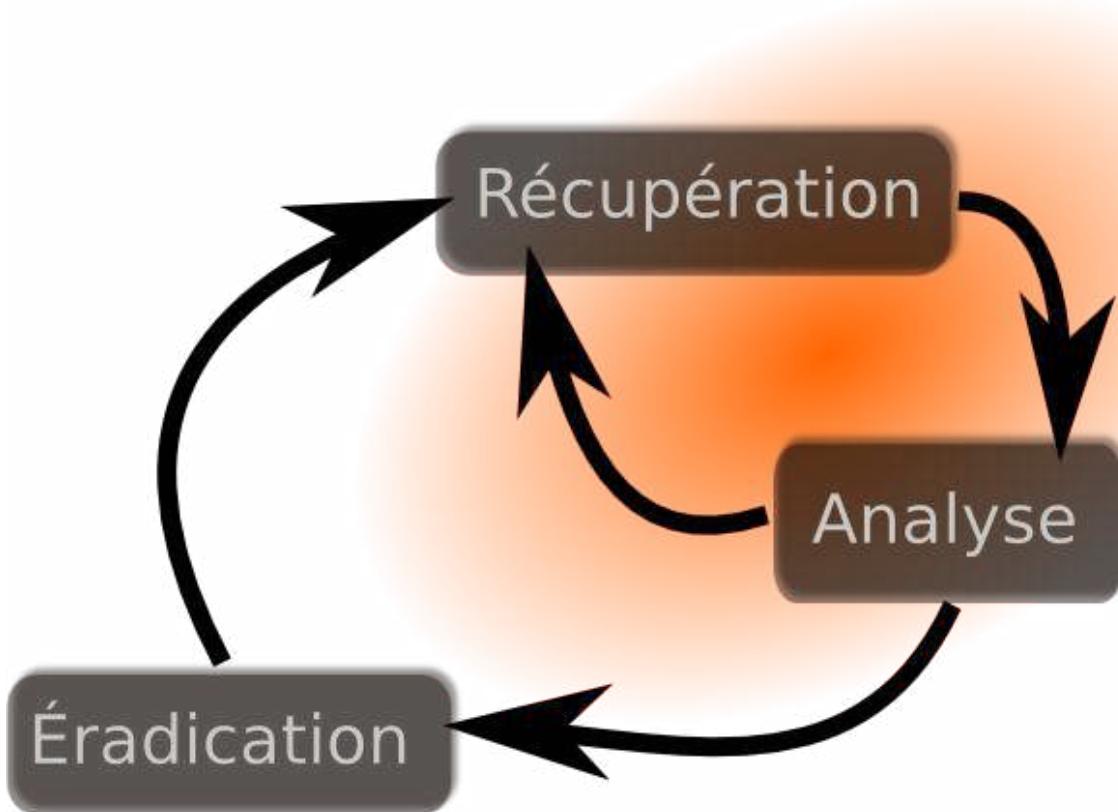
Se fait dans les bureaux des enquêteurs pour déterminer

- l'impact potentiel de l'attaque,
- l'équipe à mettre en place,
- les moyens à mettre en œuvre,
- ...

## Récupération, Analyse et Éradication

version : 06-10-2014 08:33

# Récupération



## Récupération

- Est-ce que les preuves doivent être conservées intacts ?
- Est-ce que les services peuvent être arrêtés ?
- Quels sont le temps et les ressources nécessaires ?
- Quels est le temps nécessaire pour appliquer la stratégie ?

Les preuves :

- doivent permettre de résoudre l'incident
- peuvent être utilisées dans des procédures judiciaires
- doivent être bien documentées :

Informations d'identifications à collecter :

- personne qui a collectée la preuve
- date et heure de chaque analyse
- endroit où la preuve est stockée
- ...

# Analyse

L'analyse se fait sur une copie L'objectif est de :

- retrouver toutes les traces d'effraction
- trouver d'où vient l'attaquant (interne/externe)
- trouver qu'elle machine a été utilisée pour attaquer
- scan de son adresse IP
- recherche dans les moteurs de recherche
- utilisation des bases de données d'incidents
- surveillance de l'activité de l'attaquant

# Éradication

Suppression des

- virus
- cheval de troie
- backdoors
- comptes vérolés et
- vulnérabilités

En faisant :

- Ré-installation via un backup
- Ré-installation « from scratch »
- Modifications des routes du réseau
- Changement des mots de passe
- ...

# Post-Incident

version : 06-10-2014 08:34

Objectif : Apprendre et Améliorer

Cela peut-être une réunion et/ou un rapport :

- relater ce qui s'est passé
- résumer la gestion de l'incident
- lister les informations qui auraient pu être dispo avant

- lister les actions qui ont pu entraver l'analyse
- lister les actions qui auraient pu accélérer l'analyse
- lister les informations qui auraient pu être partagées
- lister les actions correctives pour le SI
- lister les outils supplémentaires qui auraient pu aider

## 3.5) Exemples de réponse à un incident

version : 17-02-2017 11:03

### Stuxnet

- Historique de Stuxnet
- Technologies utilisées par Stuxnet

### TV5 Monde

- TV5 Monde : l'attaque
- TV5 Monde : la résolution

### Historique de Stuxnet

version : 08-01-2015 21:42

<http://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf>

- **17 juin 2010**, lorsque la société biélorusse Virusblokada publie un rapport sur le virus RootkitTmphider, faisant mention de la faille de sécurité LNK
- **14 juillet**, le MITRE assignait les références CVE-2010-2729 et CVE-2010-2743 aux failles de sécurité présentes dans le spouleur d'impression ainsi que dans la gestion du clavier
- **16 juillet**, Microsoft publie une alerte de sécurité référencée KB2286198
- **17 juillet**, Symantec renommait W32.Temphid en W32.Stuxnet et Siemens rapportait que la société était en train d'étudier des rapports évoquant la compromission de plusieurs systèmes SCADA couplés à WinCC

- **19 juillet**, IvanLeFou et HD Moore produisent des preuves de concepts de la vulnérabilité LNK
- **20 juillet**, Symantec annonçait avoir découvert comment le malware échangeait avec les serveurs de commandes et de contrôle (C&C) ainsi que la signification des messages échangés.
- **21 juillet**, le MITRE assignait la référence CVE-2010-2772 à la faille de sécurité présente au sein des logiciels Simatic WinCC et PCS 7 de Siemens
- **14 septembre**, le MITRE assignait la référence CVE-2010-3338 à la vulnérabilité de type élévation de privilèges identifiée au sein du planificateur de tâches
- **16 septembre**, Langner annonce que l'Iran, et plus particulièrement la centrale nucléaire de Bushehr qui a été construite en coopération avec la Russie, serait principalement visée
- **30 septembre**, ESET et Symantec ont publié une première version de leur rapport présentant leurs analyses (presque) complètes du malware
- **15 novembre**, Langner présente une solution technique qui permet au code malveillant 315 de détruire des centrifugeuses à gaz de Natanz et une description détaillée du code 417 ciblant les turbines à vapeur de la centrale de production électrique de Bushehr.

## Technologies utilisées par Stuxnet

version : 06-10-2014 08:35

Il y a 2 fonctions principales dans ce vers :

1. la propagation du virus, qui repose sur des failles inhérentes à la plateforme Windows,
  - utilisation de la faille LNK et le bon vouloir des utilisateurs
  - utilisation d'une faille dans le Spouleur d'impression Windows
  - utilisation d'une vieille faille de sécurité ~MS08-067 du Service Serveur (dépôt d'un fichier dans les partages du type C\$ ou Admin\$)
  - installation d'un serveur RPC pour que les différentes parties du vers puissent communiquer
  - élévation de privilèges :
    - via une faille dans la gestion du clavier par le pilote "Win32k.sys" (Windows 2000 et XP)
    - via une faille du planificateur de tâches (Windows Vista, 7 et 2008)
  - camouflage via un rootkit

## 2. l'attaque des systèmes SCADA articulés autour de WinCC et de ~PCS7

- injection de commandes SQL
- recherche de deux types d'appareil portant les références Siemens 6ES7-315- et 6ES7-417
- injection de code malveillants capable de se camoufler de la vue des superviseurs
- envoi de données aléatoires pendant 50 minutes environ puis redonne la main au système nominal (qui va travailler normalement entre 13 jours et 3 mois)

# TV5 Monde : l'attaque

version : 17-02-2017 11:02

Le 8 avril 2015 à 20 h 50 HAEC, l'infrastructure de diffusion de TV5 Monde (le multiplexage) est la cible d'une cyberattaque. Même si l'infrastructure principale et celle de secours sont neutralisées d'un seul coup, le directeur informatique de la chaîne et son équipe croient tout d'abord à une panne technique. Mais quelques minutes plus tard, le serveur de messagerie électronique est détruit, confirmant une cyberattaque.

Pour limiter les dégâts, les équipes techniques coupent l'ensemble du réseau informatique vers 22 h, interrompant les diffusions télévisées de la chaîne dans le monde.

En parallèle, les comptes Twitter et Facebook de la chaîne sont également piratés. Des messages de soutien à l'État islamique en anglais, arabe et français y sont publiés, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI.

Peu avant minuit, les équipes techniques arrivent à reprendre le contrôle des réseaux sociaux et postent des messages d'explication à destination des internautes. Le directeur général de TV5 Monde, Yves Bigot, poste une vidéo sur Facebook et parle d'une « cyberattaque extrêmement puissante ».

Le 9 avril à partir de 5 h HAEC, le système informatique et les signaux télévisés sont progressivement relancés.

via [https://fr.wikipedia.org/wiki/Cyberattaque\\_contre\\_TV5\\_Monde](https://fr.wikipedia.org/wiki/Cyberattaque_contre_TV5_Monde)

# TV5 Monde : la résolution

version : 17-02-2017 11:08

## 9 avril 2015

le parquet de Paris saisit la direction générale de la Sécurité intérieure (DGSI), la sous-direction anti-terroriste (SDAT), et les cyber-policiers de la direction centrale de la Police judiciaire (DCPJ)

## 10 avril

le ministère de la défense annonce qu'aucun document confidentiel relatif à l'armée française et à l'identité de militaires et de leur famille n'a été diffusée

## 13 avril

les autorités confirment que l'attaque n'a pu être perpétrée par un seul individu mais par un groupe de plusieurs dizaines de pirates de haute volée, qui ont pu être engagés comme mercenaires.

- les pirates ont utilisé la technique de l'hameçonnage (ou phishing) en envoyant un e-mail fin janvier à l'ensemble des journalistes de la chaîne.
- 3 d'entre eux ont répondu, permettant aux hackers de pénétrer le réseau de la chaîne via un cheval de Troie.
- 3 semaines avant l'attaque, un virus informatique s'est propagé dans plusieurs ordinateurs, profitant d'une architecture informatique mélangeant la partie « métier » constituant le cœur de la chaîne et la partie bureautique ouverte sur l'extérieur via Internet.
- les pirates auraient créé des comptes avec des droits d'administrateurs leur permettant de circuler là où ils le souhaitaient

## juin

les médias révèlent que l'enquête s'éloigne de la piste djihadiste, vue comme un leurre, et s'oriente vers celle d'un groupe de hackers russes nommé APT28 (aussi connu sous le nom de Pawn Storm, Tsar Team, Fancy Bear ou Sednit)

- La cyberattaque présenterait des similitudes avec le mode opératoire de ce groupe,
- utiliserait des serveurs communs et
- le code source aurait été tapé sur un clavier cyrillique à des moments correspondant aux heures de bureau à Saint-Pétersbourg et à Moscou

## 4) Techniques

version : 04-11-2014 21:58

### TableOfContents

Sommaire :

- Généralités
- Dead Forensics
- Live Forensics
- Network Forensics
- Social Forensics
- Cloud Forensics

## 4.1) Techniques Généralités

version : 06-10-2014 08:36

- Préparer l'analyse
- Faire des images des preuves
- Emmener les preuves
- Préparer les preuves
- Examiner les preuves

## 4.2) Techniques Dead Forensics

version : 21-12-2014 20:52

Description des technologies des disques durs

## Récupération des données

- Copie bit-à-bit de disque
- Copie d'image virtuelle
  - Exemple : Récupération d'image VMWare

## Disques en clair

- Analyse par recherche syntaxique
- Analyse par « carving »
- Analyse de fichiers particuliers

- Fichiers de configuration
  - Exemple .bash\_history
- Fichiers d'audit
  - Exemple Apache
  - Analyse suivant la timeline
- Correspondances
  - Exemple Correspondance Mail
- Fichiers de type image
- Exécutables (retro)
- Base de registre
- Shellbags
- Autres fichiers
  - Corrélation applications / Fichiers ouverts
  - Exemple Scripts basés sur PowerShell
- Bases de données
- Analyse par couches
- Stéganographie

## Disques chiffrés

### Technologies de chiffrement

- déchiffrer le disque
  - en utilisant une vulnérabilité dans l'outil de chiffrement
  - en récupérant la clé de chiffrement
    - caché quelque part sur un média
    - caché quelque part sur un bout de papier
    - stocké en RAM

## Description des technologies des disques durs

version : 08-01-2015 22:42

Un historique des tailles de disques durs toutes technologies confondues (via [http://fr.wikipedia.org/wiki/Disque\\_dur](http://fr.wikipedia.org/wiki/Disque_dur))

Date	Fabricant	Modèle	Taille
4 To	2011	Hitachi 7K4000	3,5"
3 To	2010	Seagate	3,5"

2 To	2009	Western Digital Caviar Green ~WD20EADS	3,5"
1 To	2007	Hitachi Deskstar 7K1000	3,5"
500 Go	2005	Hitachi	3,5"
25 Go	1998	IBM Deskstar 25 GP	7,0"
1,02 Go	1982	Hitachi H8598	14"
28 Mo	1962	IBM modèle 1301	
5 Mo	1956	IBM 305 Ramac	24"

Disques durs classiques

Solid State Drive et mémoire flash

Disques durs hybrides

## Disques durs classiques

version : 08-01-2015 22:45

[http://fr.wikipedia.org/wiki/Disque\\_dur](http://fr.wikipedia.org/wiki/Disque_dur)

## Description

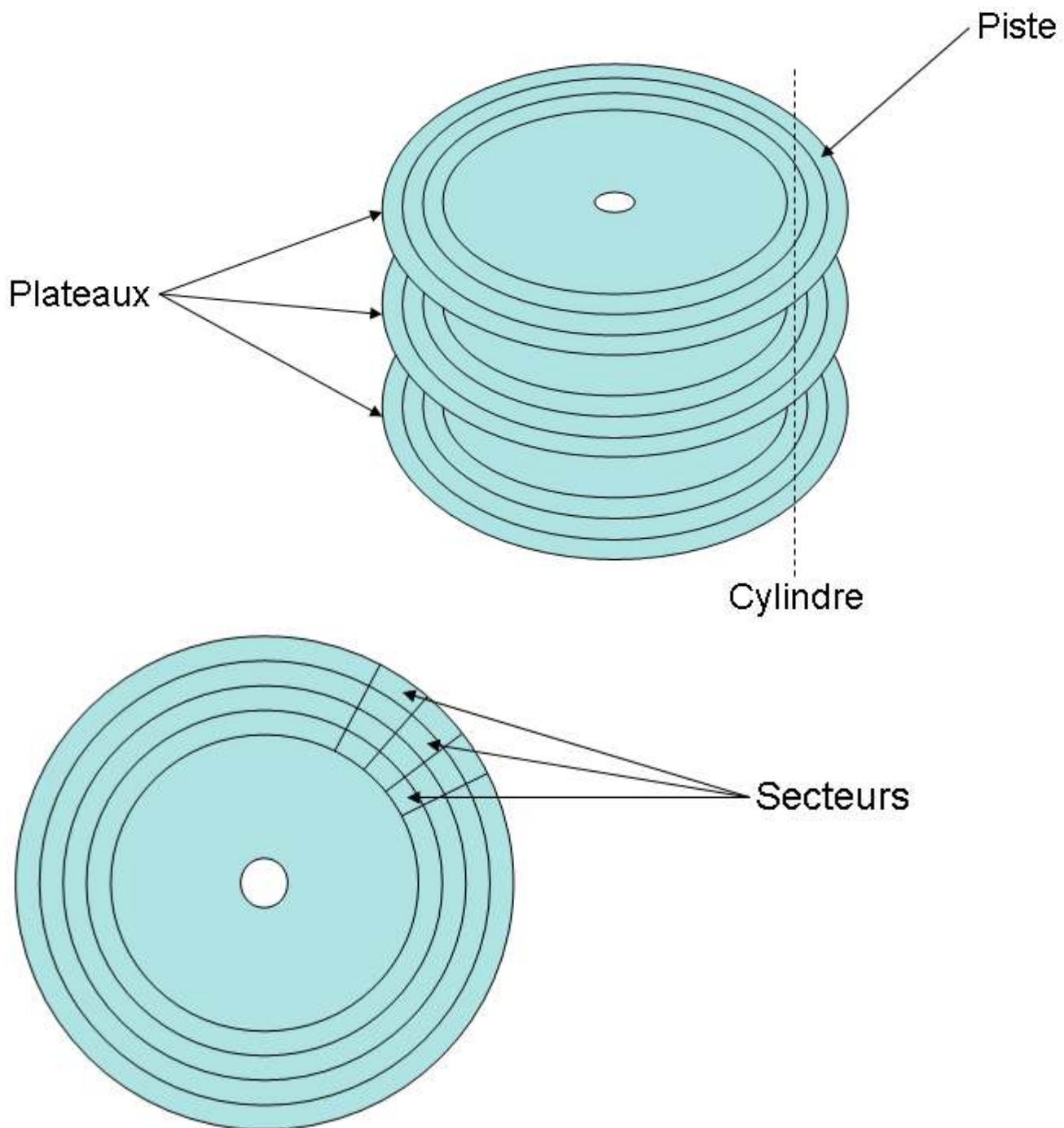


Un disque dur est constitué :

- de **plateaux** (aluminium, céramique, verre) paramagnétiques
- ces plateaux tournent autour d'un **axe**
- un (ou plusieurs) **bras** vient positionner
- une **tête** de lecture sur les plateaux (déplacement radial par rapport aux plateaux)
- un contrôleur de disque qui a pour mission :
  - de piloter les moteurs de rotation
  - de piloter le déplacement des têtes de lecture/enregistrement
  - d'interpréter les signaux électriques

La vitesse de rotation des plateaux est constante et la tête de lecture vient *imprimer* des "0" et des "1" à la surface du plateau. La vitesse typique de rotation des disques : \* 3 600, 4 200, 5 400, 7 200, 10 000 et 15 000 tours par minute

## Géométrie



En adressage **CHS**, il faut 3 coordonnées pour accéder à un bloc (ou secteur) de disque :

1. le numéro de la piste (détermine la position du bras portant l'ensemble des têtes) ;
2. le numéro de la tête de lecture (choix de la surface) ;
3. le numéro du bloc (ou secteur) sur cette piste (détermine à partir de quel endroit il faut commencer à lire les données).

Chaque secteur est composé de 5 parties :



# Solid State Drive et mémoire flash

version : 08-01-2015 22:50

[http://fr.wikipedia.org/wiki/Solid\\_State\\_Drive](http://fr.wikipedia.org/wiki/Solid_State_Drive)

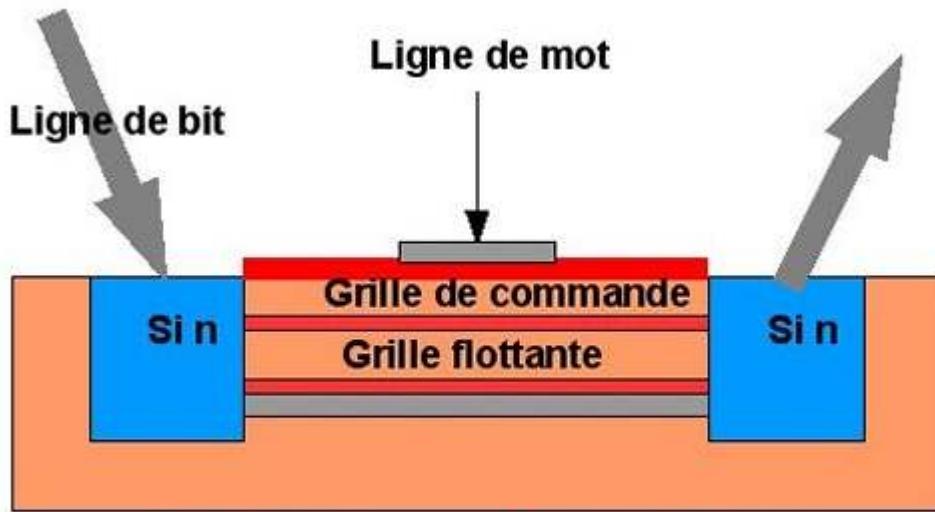
Avantages par rapport aux disques durs classiques:

- moins fragiles ;
- moins bruyant lors des lectures de données ;
- moins de latences pour l'accès aux données.

Inconvénients :

- usure rapide de la capacité de stockage
- coupures de courant qui peuvent rendre le contenu du lecteur irrécupérable

**Les SSD sont des mémoires flash**



**Cellule d'une mémoire flash**

La véritable donnée est contenue dans la grille flottante :

- une grille déchargée correspond à un "1" binaire
- une grille chargée correspond à un "0" binaire

La lecture se fait par la ligne de bit en envoyant une certaine tension  
L'écriture se fait par la ligne de mot :

- soit on charge la ligne de mot et la ligne de bit
- soit on décharge via un courant négatif dans la grille de commande

(cf. [http://www.feb-patrimoine.com/nsdat/mediatheque/expos/mam\\_2008/Borne\\_MAM/11.html](http://www.feb-patrimoine.com/nsdat/mediatheque/expos/mam_2008/Borne_MAM/11.html))

Il existe trois types de mémoire flash :

- la SLC NAND (Single Level Cell),
  - 1 cellule = 1 bit (2 niveaux de charge),
- la MLC NAND (Multi Level Cell),
  - 1 cellule = 2 bit (4 niveaux de charge),
- la TLC NAND (Triple Level Cell),
  - 1 cellule = 3 bit (8 niveaux de charge)

La commande TRIM permet à un système d'exploitation (Linux, Windows) d'indiquer à un contrôleur de disque de type mémoire flash quels blocs de données ne sont plus utilisés et peuvent donc être effacés.

## Disques durs hybrides

version : 08-01-2015 22:51

On trouve depuis quelques temps des disques dit hybrides

Ces disques sont constitués :

- d'un disque dur *traditionnel* (typiquement 1To) et
- d'une mémoire cache non volatile de type Flash.

Le contrôleur de ces disques est très spécifique.

## Récupération d'image VMWare

version : 19-11-2014 21:08

Montage du disque VMWare :

```
$ affuse CNT926C1flat.vmdk mount/
```

Récupération des informations du disque virtuel :

```
$ mmls t dos mount/CNT926C1flat.vmdk.raw
DOS Partition Table
Offset Sector: 0
Units are in 512byte sectors
      Slot    Start          End          Length
Description
00: Meta    0000000000    0000000000    0000000001
Primary Table (#0)
01:        0000000000    0000000062    0000000063
Unallocated
02: 00:00    0000000063    0030041549    0030041487
Linux (0x83)
03: Meta    0030041550    0031455269    0001413720
DOS Extended (0x05)
04: Meta    0030041550    0030041550    0000000001
Extended Table (#1)
05:        0030041550    0030041612    0000000063
Unallocated
06: 01:00    0030041613    0031455269    0001413657
Linux Swap / Solaris x86 (0x82)
07:        0031455270    0031457279    0000002010
Unallocated
```

Copie de la partition Linux :

```
$ mmcatt mount/CNT926C1flat.vmdk.raw 2 > linux.raw
```

Recherche de données concernant les fichiers supprimés sur /var/www :

```
$ fls dr linux.raw | grep "var/www"
...
r/r * 793398:
var/www/.bash_history.swp
r/r * 793697:
var/www/.bash_history.swx
```

```
r/r * 793705:  
var/www/bash  
r/r * 793389:  
var/www/.bash_history  
r/r * 793706:  
var/www/sh  
r/r * 793707:  
var/www/sh.1  
r/r * 793398:  
var/www/.bash.swp  
r/r * 793704:  
var/www/.bash.swpx
```

## Exemple .bash\_history

version : 12-10-2014 17:39

```
...  
ls  
id  
cd /etc  
echo "systeme:x:20:0:root:/root:/bin/bash" >> passwd  
echo "systeme:Q,Jpl.or6u2e7:10795:0:99999:7:-  
1:-1:134537220" >> shadow  
su - systeme  
...
```

## Exemple Apache

version : 12-10-2014 17:40

```
[Wed Nov 13 21:07:31.505873 2013] [core:notice] [pid  
4329:tid 3074087488] AH00094: Command line: '/usr/sbin  
/apache2'  
[Wed Nov 13 22:14:29.456459 2013] [mpm_worker:notice]  
[pid 4329:tid 3074087488] AH00295: caught SIGTERM,  
shutting down  
[Thu Nov 14 06:58:53.700993 2013] [mpm_worker:notice]  
[pid 3565:tid 3073870400] AH00292: Apache/2.4.6 (Ubuntu)  
OpenSSL/1.0.1e configured -- resuming normal operations  
[Thu Nov 14 06:58:53.713728 2013] [core:notice] [pid
```

```
3565:tid 3073870400] AH00094: Command line: '/usr/sbin  
/apache2'
```

## Analyse suivant la timeline

version : 08-01-2015 22:21

TODO : <http://journeyintoir.blogspot.fr/2014/10/timeline-analysis-by-categories.html>

La corrélation temporelle est importante pour découvrir les actions des attaquants sur les systèmes compromis.

Le challenge de la corrélation repose sur les principes suivants :

- 2 fichiers de logs ne s'appuient pas forcément sur la même date
- les fichiers de logs n'ont pas obligatoirement la même précision au niveau du temps
- les fichiers de logs n'ont pas la même structure
- les informations intéressantes ne sont pas systématiquement dans des fichiers

## Exemple Correspondance Mail

version : 12-10-2014 17:41

E-mail Attachments

Description:

The e-mail industry estimates that 80% of e-mail data is stored via attachments. E-mail standards only allow text. Attachments must be encoded with MIME / base64 format.

Location:

Outlook XP

```
%USERPROFILE%\Local Settings\Application Data\Microsoft  
\Outlook
```

Win7

%USERPROFILE%\AppData\Local\Microsoft\Outlook

Interpretation:

MS Outlook data files found in these locations include OST and PST files. One should also check the OLK and Content.Outlook folder which might roam depending on the specific version of Outlook used. For more information on where to find the OLK folder this link has a handy chart:

<http://www.hancockcomputertech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-olk-folder>

## Fichiers de type image

version :

Missing tiddler "Fichiers de type image" - click  to create

## Base de registre

version : 12-10-2014 17:44

Dead Forensics

Techniques

source : <http://journeyintoir.blogspot.fr/2011/07/obtaining-information-about-operating.html>

voir aussi : <http://www.4n6k.com/2013/05/userassist-forensics-timelines.html?m=1>

## General Operating System Information

- Operating system version and product name (HKLM\Software\Microsoft\Windows NT\Currentversion)
- Registration information for owner and organization entered during installation (HKLM\Software\Microsoft\Windows NT\Currentversion)
- Machine Security Identifier (SID) (HKLM\Security\Policy\PolAcDms)
- Shutdown information (HKLM\System\Controlset###\Control\Windows)
- Timezone information (HKLM\System\Currentcontrolset\Control\Timezoneinformation)
- Auditing configuration (HKLM\Security\Policy\PolAdtEv)

- Determine if the NTFS last access time is set to not to update (HKLM\System\CurrentControlSet\Control\Filesystem\NtfsDisableLastAccessUpdate)

## User Account Information

- Configured local user accounts and groups (HKLM\SAM\Domains\Account)
- User profiles on machine and registered with Windows (Profilelist registry key)
- Logon username of the specified user account (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer)
- Previous user accounts to log onto the machine (HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Defaultusername and HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Altdevaultusername)

## Software Information

- Programs showed on the Add/Remove Programs control panel applet (HKLM\Software\Microsoft\Windows\Currentversion\Uninstall)
- File system paths to various programs (HKLM\Software\Microsoft\Windows\Currentversion\App paths)
- Information about installed products (HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\UserData)
- Default web browser (one area to check is HKLM\Software\Classes\HTTP\shell\open\command)
- User specific software (HCU\Software)
- User activity via the Windows Explorer shell may show programs ran (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist)
- Executables associated with the user account (XP is HKCU\Software\Microsoft\Windows\Shell\NoRoam\~MUICache and Vista/7 is is HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache in userclass.dat)

## Networking Information

- Computer name (HKLM\System\Currentcontrolset\Control\Computername)
- Domain and hostname (HKLM\System\~Currentcontrolset\Services\Tcpip\Parameter)
- Configured network shares on the computer (HKLM\System\Currentcontrolset\Services\Lanmanserver\Shares)
- Configured persistent routes (HKLM\System\ControlSet###\Services\Tcpip\Parameters\PersistentRoutes)
- Firewall configuration (HKLM\System\Currentcontrolset###\Services\Sharedaccess\Parameters\Firewallpolicy)
- Networking information (HKLM\System\Currentcontrolset###\Network)
- Cache of computers seen by Windows Explorer (HKCU\Software\Microsoft\Windows\Currentversion\Explorer\Computerdescriptions)

## Storage Location Information

- Devices and volumes mounted to the computer (HKLM\System\MountedDevices)
- Location of the user account profile folders (HKCU\Software\Microsoft\Windows\Currentversion\Explorer\User shell folders)
- Map network drives available to a user (HKCU\Software\Microsoft\Windows\Currentversion\Explorer\Map network drive MRU)
- Volumes mounted by a user (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2)

## Acrobat Reader

via <http://dereknewton.com/category/windows-forensics/>

Acrobat Reader sauvegarde certaines données dans la base de registre et notamment :

- les 5 fichiers ouverts récemment : Software\Adobe\~AVGeneral\cRecentFiles

et on peut récupérer la date de la dernière ouverture du dernier fichier en regardant la date de modification de cette clé de registre

## Shellbags

version : 08-01-2015 22:26

<http://williballenthin.com/forensics/shellbags/index.html>

Microsoft Windows utilise un ensemble de **clés de registre** appelés «shellbags» pour enregistrer la taille, l'affichage, l'icône, et la position d'un dossier lorsque l'on utilise Explorer. Ces clefs sont utiles à un enquêteur judiciaire. Les informations des Shellbags sont **persistentes**, même après la **suppression des répertoires**, ce qui signifie qu'ils peuvent être utilisés pour énumérer passé les volumes montés, les fichiers supprimés et les actions de l'utilisateur.

## Localisation des shellbags :

Windows XP system :

- HKEY\ USERS\{USERID}\Software\Microsoft\Windows\Shell\
- HKEY\ USERS\{USERID}\Software\Microsoft\Windows\ShellNoRoam\

La clé de registre HKEY\ USERS\{USERID\} est persistante dans le fichier NTUser.dat.

Windows 7 system :

- HKEY\ USERS\{USERID}\Local Settings\Software\Microsoft\Windows\Shell\

La clé de registre HKEY\ USERS\{USERID\} est persistante dans le fichier UsrClass.dat.

## Corrélation applications / Fichiers ouverts

version : 12-10-2014 17:44

Dead Forensics

Techniques

<http://windowsir.blogspot.fr/2013/07/howto-correlate-files-to-application.html>

- Convention de nommage (DSC..., IMG...)
- Recherche dans le répertoire %Temp%
- Analyse des premiers octets d'un fichier (utilisation d'un éditeur hexa)
- Analyse des metadatas
- Analyse des "dossiers de décharge" (*folder dumps*) cf. Cédric Pernet
- Analyse des "flux de données alternatifs NTFS" (*NTFS Alternate Data Streams*) cf. windowsir
- Chronologie des événements

## Exemple Scripts basés sur PowerShell

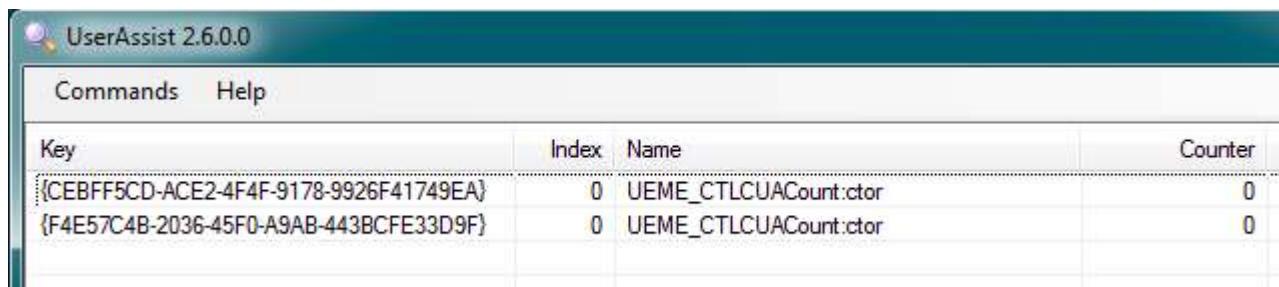
version : 12-10-2014 17:45

Source [blog.s21sec.com](http://blog.s21sec.com)

PowerShell est une interface de script avancé pour Windows. Il est inclus par défaut avec Windows 7, 2008 et supérieur.

Lorsqu'on lance un script PowerShell, le système d'exploitation effectue les modifications suivantes :

- mise à jour de clés de registre: (UserAssist)



Key	Index	Name	Counter
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	0	UEME_CTLCUACount:ctor	0
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	0	UEME_CTLCUACount:ctor	0

- création d'une série d'événements dans les journaux de service (section "Windows PowerShell")

Screenshot of Event Viewer (Local) showing Windows PowerShell events.

**Windows PowerShell** Number of events: 10

Level	Date and Time	Source	Event ID	Task Category
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	1/11/2013 3:13:09 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Event 600, PowerShell (PowerShell)

**General** **Details**

Provider "Environment" is Started.

Details:

```

ProviderName=Environment
NewProviderState=Started

SequenceNumber=3

HostName=ConsoleHost
HostVersion=2.0
HostId=d07dd3b1-351d-4e07-8cf0-baf1ddc6c7f1
EngineVersion=

```

- création de fichiers temporaires %TEMP%

	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.tmp	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.0.cs	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.dll	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.cmdline	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.out	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.err	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.out	SUCCESS
	powershell.exe	1780		C:\Users\usuario\AppData\Local\Temp\q_zp5th8.dll	SUCCESS

## Bases de données

version : 08-01-2015 22:32

Comment modifier un mot de passe de la base de données MySQL :

```

vdsq3226@vdsq3226-mobile:~/ $ sudo service mysql stop
mysql stop/waiting
vdsq3226@vdsq3226-mobile:~/ $ sudo /usr/bin/mysqld_safe
--skip-grant-tables &
[2] 12526
vdsq3226@vdsq3226-mobile:~/ $ 131216 13:55:56
mysqld_safe Can't log to error log and syslog at the
same time. Remove all --log-error configuration
options for --syslog to take effect.

```

```
131216 13:55:56 mysqld_safe Logging to '/var/log/mysql/error.log'.
131216 13:55:57 mysqld_safe Starting mysqld daemon
with databases from /var/lib/mysql
```

```
vdsq3226@vdsq3226-mobile:~/$
vdsq3226@vdsq3226-mobile:~/$ mysql -h localhost
Welcome to the MySQL monitor.  Commands end with ; or
\g.
Your MySQL connection id is 1
Server version: 5.5.34-0ubuntu0.13.10.1-log (Ubuntu)
```

Copyright (c) 2000, 2013, Oracle and/or its  
affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation  
and/or its  
affiliates. Other names may be trademarks of their  
respective  
owners.

Type '**help;**' or '**\h**' for help. Type '**\c**' to clear the  
current input statement.

```
mysql> select user,host from mysql.user;
+-----+-----+
| user      | host       |
+-----+-----+
| root      | %          |
| ufcollector | %          |
| root      | 127.0.0.1  |
| root      | ::1        |
|          | localhost   |
| debian-sys-maint | localhost |
| root      | localhost   |
| ufcollector | localhost   |
|          | vdsq3226-mobile |
| root      | vdsq3226-mobile |
+-----+-----+
10 rows in set (0.00 sec)
```

```
mysql> use mysql;
```

```
Reading table information for completion of table and
column names
You can turn off this feature to get a quicker startup
with -A
```

Database changed

```
mysql> update user
      -> set password=password('monmotdepasse')
      -> where user='root' and host='localhost';
Query OK, 1 row affected (0.03 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

```
mysql> quit
```

Bye

```
vdsq3226@vdsq3226-mobile:~/ $ sudo mysqladmin shutdown
vdsq3226@vdsq3226-mobile:~/ $ 131216 13:57:59
mysqld_safe mysqld from pid file /var/run/mysqld
/mysqld.pid ended
```

```
[2]+ Fini                  sudo /usr/bin
/mysqld_safe --skip-grant-tables
vdsq3226@vdsq3226-mobile:~/ $
vdsq3226@vdsq3226-mobile:~/ $ sudo service mysql start
mysql start/running, process 12992
vdsq3226@vdsq3226-mobile:~/ $ mysql -uroot
-pmonmotdepasse
Welcome to the MySQL monitor.  Commands end with ; or
\g.
Your MySQL connection id is 36
Server version: 5.5.34-0ubuntu0.13.10.1-log (Ubuntu)
```

Copyright (c) 2000, 2013, Oracle and/or its  
affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation  
and/or its  
affiliates. Other names may be trademarks of their  
respective  
owners.

Type '**help;**' or '**\h**' for help. Type '**\c**' to clear the  
current input statement.

```
mysql> select user,host from mysql.user;
+-----+-----+
| user      | host       |
+-----+-----+
| root      | %          |
| ufcollector | %          |
| root      | 127.0.0.1  |
| root      | ::1        |
|          | localhost   |
| debian-sys-maint | localhost |
| root      | localhost   |
| ufcollector | localhost   |
|          | vdsq3226-mobile |
| root      | vdsq3226-mobile |
+-----+-----+
10 rows in set (0.00 sec)

mysql> quit
Bye
vdsq3226@vdsq3226-mobile:~/
```

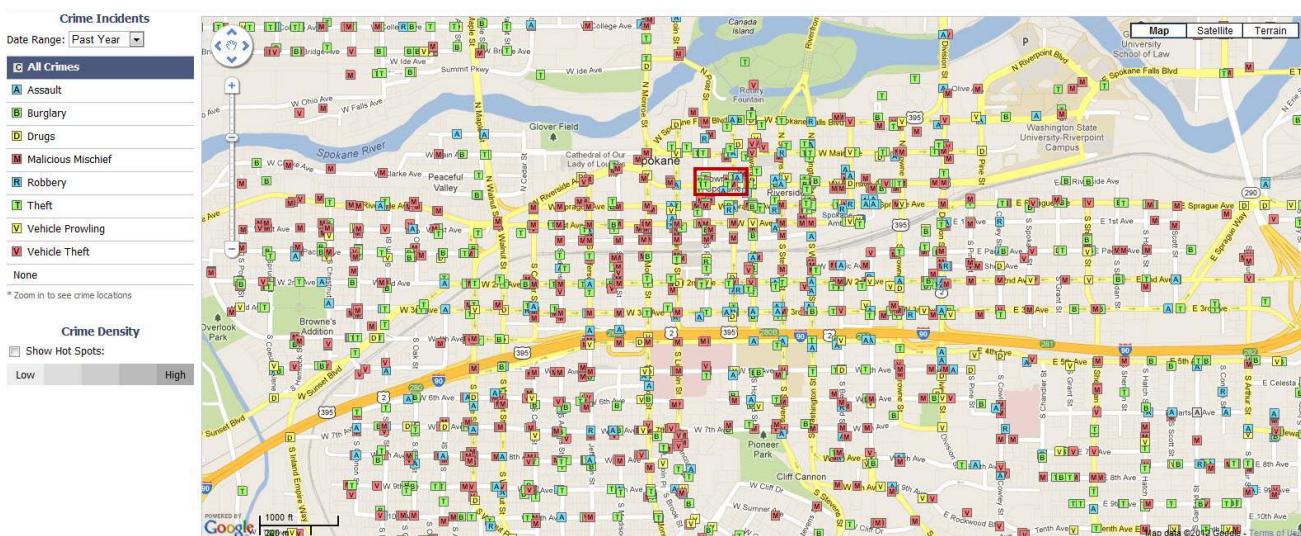
## Analyse par couches

version : 12-10-2014 17:46

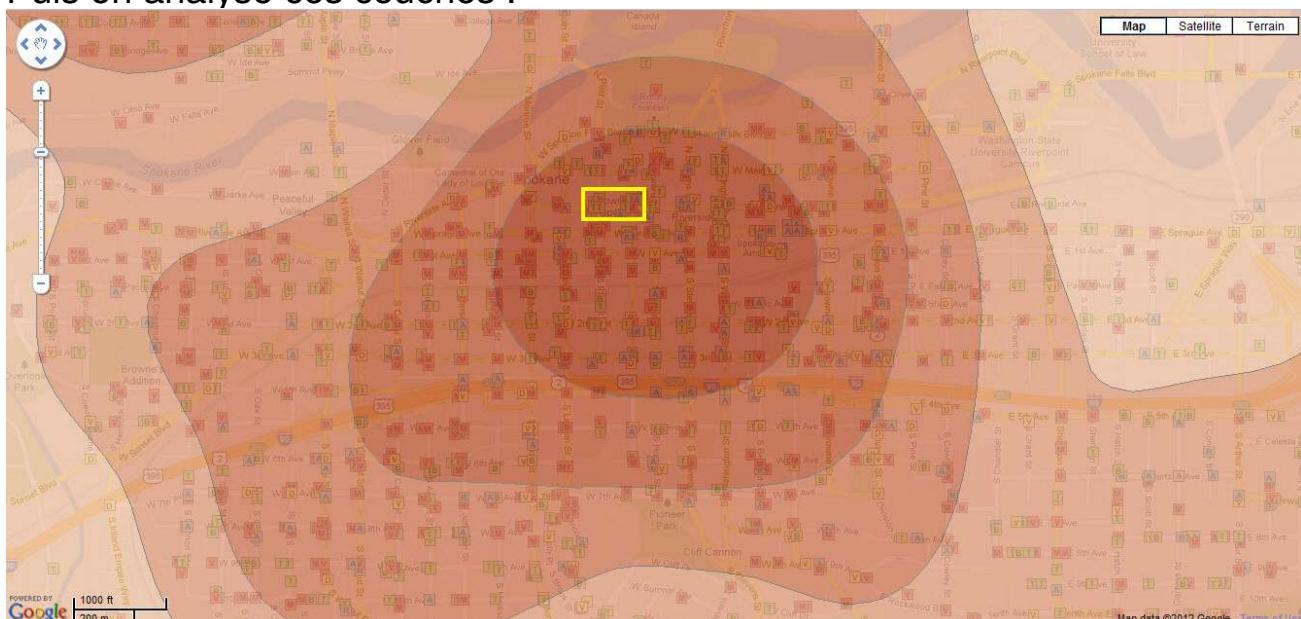
Source :

- [Layering data](#)
- [Deeper look into Windows logs](#)

Exemple de vols dans une ville, on ajoute des couches (**layers**) :



Puis on analyse ces couches :



On peut effectuer le même type d'analyse en informatique avec dans un premier temps les **NTFS Extended Attributes** dont la **Master File Table (AnalyzeMFT)** :

	A	B	D	F	G	J	K
1	date	time	MACB	sourcetype	type	short	desc
219414	12/6/2012	22:18:05...B		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/n	desc
219420	12/6/2012	22:18:06...A...		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc
219421	12/6/2012	22:18:06...M...		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc
219422	12/6/2012	22:18:06...C...		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc

En rajoutant des couches (plusieurs types de logs) comme par exemple :

- \$LogFile (*Advanced NTFS Journal Parser*)
- \$UsnJrnl (*Tzwork's Windows Journal Parser*)

on obtient ceci :

1	date	time	MACB	sourcetype	type	short	desc
219398	12/6/2012	22:18:05 ...B		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/L	desc
219399	12/6/2012	22:18:05		NTFS \$LogFile	File Rename Event	File Renamed	Renamed: servic-> - Parent: 1802
219400	12/6/2012	22:18:05		NTFS \$LogFile	File Creation Event	FILE Created	Created FILE: services.exe - Parent: 1802
219401	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_created	n	
219402	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_added	n	
219403	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	attrib_changed	n	
219404	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_added	n	
219405	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	attrib_changed	n	
219406	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_added	n	
219407	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	attrib_changed	(5da39e95-8007-4308-c6cf-bcce61795d0d)	
219408	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_created	(5da39e95-8007-4308-c6cf-bcce61795d0d)	
219409	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	attrib_changed	(5da39e95-8007-4308-c6cf-bcce61795d0d)	
219410	12/6/2012	22:18:05 ...B		NTFS:\$UsnJrnl JS	file_created	(5da39e95-8007-4308-c6cf-bcce61795d0d)	
219411	12/6/2012	22:18:05 ...A		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/n	desc
219412	12/6/2012	22:18:05 ...M		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/n	desc
219413	12/6/2012	22:18:05 ...C		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/n	desc
219414	12/6/2012	22:18:05 ...B		NTFS \$MFT	\$SI [...] time	/Windows/Installer/[5da39e95-8007-4308-c6cf-bcce61795d0d]/n	desc
219415	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	access_changed	services.exe	
219416	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	access_changed	services.exe	
219417	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	access_changed	services.exe	
219418	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	access_changed	services.exe	
219419	12/6/2012	22:18:05 ...C		NTFS:\$UsnJrnl JS	file_renamed	services.exe	
219420	12/6/2012	22:18:06 ...A		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc
219421	12/6/2012	22:18:06 ...M		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc
219422	12/6/2012	22:18:06 ...C		NTFS \$MFT	\$SI [...] time	/Windows/System32/services.exe	desc
219423	12/6/2012	22:18:06 ...C		NTFS:\$UsnJrnl JS	attrib_changed	services.exe	
219424	12/6/2012	22:18:06 ...B		NTFS:\$UsnJrnl JS	file_created	services.exe	
219425	12/6/2012	22:18:06 ...C		NTFS:\$UsnJrnl JS	attrib_changed	services.exe	
219426	12/6/2012	22:18:06 ...B		NTFS:\$UsnJrnl JS	file_added	services.exe	
219427	12/6/2012	22:18:06 ...C		NTFS:\$UsnJrnl JS	attrib_changed	services.exe	
219428	12/6/2012	22:18:06 ...B		NTFS:\$UsnJrnl JS	file_added	services.exe	

# Stéganographie

version : 12-10-2014 17:46

La détection peut se faire

- en comparant avec une base de donnée d'image
  - il faut posséder cette banque d'image
  - Encase peut le faire
- en cherchant la signature d'un logiciel donné
- en détectant des irrégularités statistiques
- en utilisant des outils de stéganalyses universelles (se basant sur des réseaux neuronaux)

Liens :

- <http://fr.wikipedia.org/wiki/St%C3%A9ganographie>
- <http://en.wikipedia.org/wiki/Steganography>
- <https://secdiary.com/creative-work-2/security-by-obscURITY-revealing-steganography/>
- [http://www.garykessler.net/library/fsc\\_stego.html](http://www.garykessler.net/library/fsc_stego.html)
- [http://www.stephan-robert.ch/attachments/File/Travaux-etudiants/\\_rapport\\_stegano.pdf](http://www.stephan-robert.ch/attachments/File/Travaux-etudiants/_rapport_stegano.pdf)
- <http://www.forensics.nl/steganography>

# Technologies de chiffrement

version : 12-10-2014 17:47

Les technologies de chiffrement les plus connues sont les suivantes :

- Truecrypt (Multi système)
- BitLocker (Windows)
- Cryptsetup et Format luks (Linux)

## 4.3) Techniques Live Forensics

version : 17-02-2017 11:10

### Système en fonction

- Analyse des variables système
  - Exemple avec ps
- Analyse des variables réseau
  - Exemple Netstat
- Analyse des fichiers ouverts
  - Exemple avec lsof
- Analyse des librairies utilisées
  - Exemple avec lsof 2
- Analyse physique

### Système éteint

- Analyse de mémoire vive
- (implique une copie préalable)

## Exemple avec ps

version : 12-10-2014 17:47

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT
START	TIME	COMMAND					
root		2	0.0	0.0	0	0	?
21:01	0:00	[kthreadd]					S
root		3	0.0	0.0	0	0	?
21:01	0:00	\_ [ksoftirqd/0]					S
root		5	0.0	0.0	0	0	?
21:01	0:00	\_ [kworker/0:0H]					S<
root		6	0.0	0.0	0	0	?
21:01	0:03	\_ [kworker/u16:0]					S
root		7	0.0	0.0	0	0	?

21:01	0:00	\_ [migration/0]				
root	8	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [rcu_bh]				
root	9	0.0 0.0	0	0 ?	S	
21:01	0:05	\_ [rcu_sched]				
root	10	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [watchdog/0]				
root	11	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [watchdog/1]				
root	12	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [migration/1]				
root	13	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [ksoftirqd/1]				
root	15	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kworker/1:0H]				
root	16	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [watchdog/2]				
root	17	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [migration/2]				
root	18	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [ksoftirqd/2]				
root	20	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kworker/2:0H]				
root	21	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [watchdog/3]				
root	22	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [migration/3]				
root	23	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [ksoftirqd/3]				
root	25	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kworker/3:0H]				
root	26	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [khelper]				
root	27	0.0 0.0	0	0 ?	S	
21:01	0:00	\_ [kdevtmpfs]				
root	28	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [netns]				
root	29	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [writeback]				
root	30	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kintegrityd]				
root	31	0.0 0.0	0	0 ?	S<	

21:01	0:00	\_ [bioset]			
root	33	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [kblockd]			
root	34	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [ata_sff]			
root	35	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [khubd]			
root	36	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [md]			
root	37	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [devfreq_wq]			
root	42	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [khungtaskd]			
root	43	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [kswapd0]			
root	44	0.0 0.0	0	0 ?	SN
21:01	0:00	\_ [ksmd]			
root	45	0.0 0.0	0	0 ?	SN
21:01	0:00	\_ [khugepaged]			
root	46	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [fsnotify_mark]			
root	47	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [ecryptfs-kthrea]			
root	48	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [crypto]			
root	60	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [kthrotld]			
root	64	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [scsi eh 0]			
root	65	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [scsi eh 1]			
root	67	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [scsi eh 2]			
root	68	0.0 0.0	0	0 ?	S
21:01	0:00	\_ [scsi eh 3]			
root	89	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [deferwq]			
root	90	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [charger_manager]			
root	142	0.0 0.0	0	0 ?	S<
21:01	0:00	\_ [firewire]			
root	233	0.0 0.0	0	0 ?	S<

21:01	0:00	\_ [kdmflush]				
root	234	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [bioset]				
root	235	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kcryptd_io]				
root	236	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kcryptd]				
root	238	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [bioset]				
root	249	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kdmflush]				
root	250	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [bioset]				
root	251	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [kdmflush]				
root	252	0.0 0.0	0	0 ?	S<	
21:01	0:00	\_ [bioset]				
root	274	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [kworker/u17:1]				
root	275	0.0 0.0	0	0 ?	S	
21:02	0:00	\_ [jbd2/dm-1-8]				
root	276	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [ext4-rsv-conver]				
root	277	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [ext4-unrsv-conv]				
root	500	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [cfg80211]				
root	531	0.0 0.0	0	0 ?	S	
21:02	0:00	\_ [irq/41-me1 me]				
root	532	0.2 0.0	0	0 ?	S	
21:02	0:19	\_ [irq/42-iwlwifi]				
root	545	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [kpsmoused]				
root	581	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [kmpathd]				
root	582	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [kmpath_handlerd]				
root	583	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [hci0]				
root	584	0.0 0.0	0	0 ?	S<	
21:02	0:00	\_ [hci0]				
root	585	0.0 0.0	0	0 ?	S<	

21:02	0:00	\_ [kworker/u17:2]				
root	586	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [hd-audio0]				
root	606	0.0 0.0	0	0	?	S
21:02	0:00	\_ [pccardd]				
root	698	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [iwlwifi]				
root	844	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [kvm-irqfd-clean]				
root	1000	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [krfcomm]				
root	1151	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [iscsi_eh]				
root	1153	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [ib_mcast]				
root	1154	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [ib_cm]				
root	1155	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [iw_cm_wq]				
root	1156	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [ib_addr]				
root	1157	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [rdma_cm]				
root	1988	0.0 0.0	0	0	?	S
21:02	0:00	\_ [kaudit]				
root	3687	0.0 0.0	0	0	?	S<
21:02	0:00	\_ [iprt]				
root	5581	0.0 0.0	0	0	?	S
22:34	0:00	\_ [kworker/u16:1]				
root	5654	0.0 0.0	0	0	?	S
22:43	0:00	\_ [kworker/u16:2]				
root	5673	0.0 0.0	0	0	?	S
22:45	0:00	\_ [kworker/2:1]				
root	5720	0.0 0.0	0	0	?	S
22:53	0:00	\_ [kworker/3:0]				
root	5744	0.0 0.0	0	0	?	S
22:55	0:00	\_ [kworker/0:0]				
root	5763	0.0 0.0	0	0	?	S
22:59	0:00	\_ [kworker/1:0]				
root	5773	0.0 0.0	0	0	?	S
22:59	0:00	\_ [kworker/3:1]				
root	5781	0.0 0.0	0	0	?	S

23:00	0:00	\_ [kworker/0:2]				
root	5796	0.0 0.0	0	0	?	S
23:02	0:00	\_ [kworker/2:2]				
root	5815	0.0 0.0	0	0	?	S
23:04	0:00	\_ [kworker/1:2]				
root	11821	0.0 0.0	0	0	?	S
23:12	0:00	\_ [kworker/u16:3]				
root	13385	0.1 0.0	0	0	?	S
23:13	0:00	\_ [kworker/0:1]				
root	1	0.0 0.0	4332	2620	?	Ss
21:01	0:01	/sbin/init				
root	312	0.0 0.0	5456	1540	?	S
21:02	0:00	mountall --daemon				
root	452	0.0 0.0	2904	872	?	S
21:02	0:00	upstart-udev-bridge --daemon				
root	456	0.0 0.0	12308	1912	?	Ss
21:02	0:00	/lib/systemd/systemd-udevd --daemon				
root	694	0.0 0.0	2884	600	?	S
21:02	0:00	upstart-socket-bridge --daemon				
102	954	0.0 0.0	4544	2192	?	Ss
21:02	0:02	dbus-daemon --system --fork				
syslog	978	0.0 0.0	31096	1384	?	Sl
21:02	0:00	rsyslogd -c5				
root	993	0.0 0.0	4864	1856	?	Ss
21:02	0:00	/usr/sbin/bluetoothd				
root	1026	0.0 0.0	3028	600	?	S
21:02	0:00	upstart-file-bridge --daemon				
root	1043	0.0 0.1	9144	6312	?	Ss
21:02	0:00	/usr/bin/perl -wT /usr/sbin/munin-node				
root	1077	0.0 0.0	3968	1692	?	Ss
21:02	0:00	/lib/systemd/systemd-logind				
avahi	1097	0.0 0.0	3616	1716	?	S
21:02	0:00	avahi-daemon: running [vdsq3226-mobile.local]				
avahi	1098	0.0 0.0	3492	432	?	S
21:02	0:00	\_ avahi-daemon: chroot helper				
root	1138	0.0 0.1	9532	4856	?	Ss
21:02	0:00	/usr/sbin/cupsd -F				
root	1159	0.0 0.0	2908	476	?	Ss
21:02	0:00	/usr/sbin/iscsid				
root	1160	0.0 0.0	3368	3224	?	S<Ls
21:02	0:01	/usr/sbin/iscsid				

```
root      1370  0.0  0.1  43228  5676 ?          Ssl
21:02  0:01 NetworkManager
root      2013  0.0  0.0   5536  3060 ?          S
21:02  0:00 \_ /sbin/dhclient -d -sf /usr/lib
NetworkManager/nm-dhcp-client.action -pf
/run/sendsigs.omit.d/network-manager.dhclient-wlan0.pid
-lf /var/lib/NetworkManager/dhclient-480b70e2-df3c-42b4-
b724-fc23ff50e88d-wlan0.lease -cf /var/lib
NetworkManager/dhclient-wlan0.conf wlan0
nobody    2137  0.0  0.0   5600  1488 ?          S
21:02  0:01 \_ /usr/sbin/dnsmasq --no-resolv --keep-
in-foreground --no-hosts --bind-interfaces --pid-
file=/var/run/NetworkManager/dnsmasq.pid --listen-
address=127.0.1.1 --conf-file=/var/run/NetworkManager
/dnsmasq.conf --cache-size=0 --proxy-dnssec --enable-
dbus=org.freedesktop.NetworkManager.dnsmasq --conf-
dir=/etc/NetworkManager/dnsmasq.d
root      1378  0.0  0.1  35340  4308 ?          Sl
21:02  0:00 /usr/lib/polkit-1/polkitd --no-debug
colord    1439  0.0  0.1  36788  5024 ?          Sl
21:02  0:00 /usr/lib/colord/colord
root      1613  0.0  0.0   4668   860  tty4      Ss+
21:02  0:00 /sbin/getty -8 38400  tty4
root      1618  0.0  0.0   4668   868  tty5      Ss+
21:02  0:00 /sbin/getty -8 38400  tty5
root      1629  0.0  0.0   4668   864  tty2      Ss+
21:02  0:00 /sbin/getty -8 38400  tty2
root      1630  0.0  0.0   4668   864  tty3      Ss+
21:02  0:00 /sbin/getty -8 38400  tty3
root      1634  0.0  0.0   4668   864  tty6      Ss+
21:02  0:00 /sbin/getty -8 38400  tty6
root      1671  0.0  0.0   7544   2460 ?          Ss
21:02  0:00 /usr/sbin/sshd -D
root      1673  0.0  0.0   8628   2772 ?          Ss
21:02  0:00 /usr/sbin/cups-browsed
root      1711  0.0  0.0   2216   628 ?          Ss
21:02  0:00 acpid -c /etc/acpi/events -s /var/run
/acpid.socket
root      1741  0.0  0.0   3168   964 ?          Ss
21:02  0:00 cron
root      1745  0.0  0.0   34988  3136 ?          SLs
21:02  0:00 lightdm
```

```
root      1769  3.9  1.7 176308 70236  tty7      Ssl+
21:02  5:12  \_ /usr/bin/X -core :0 -auth /var/run
/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
root      2878  0.0  0.0 17456   3420 ?      Sl
21:02  0:00  \_ lightdm --session-child 12 21
vdsq3226 3900  0.0  0.0   5908  2112 ?      Ss
21:03  0:00      \_ init --user
vdsq3226 3980  0.0  0.0    4144   204 ?      Ss
21:03  0:00      \_ ssh-agent
vdsq3226 3983  0.0  0.0    5300   388 ?      Ss
21:03  0:00      \_ gpg-agent --daemon --sh
vdsq3226 3987  0.0  0.0    5720   2364 ?      Ss
21:03  0:01      \_ dbus-daemon --fork --session
--address=unix:abstract=/tmp/dbus-zuJUndsZ7H
vdsq3226 3993  0.0  0.0    4968   1052 ?      Ss
21:03  0:00      \_ upstart-event-bridge
vdsq3226 3996  0.0  0.0   33412  3744 ?      Ss
21:03  0:00      \_ /usr/lib/i386-linux-gnu/hud
/window-stack-bridge
vdsq3226 4011  0.2  0.1  46920   4044 ?      Ssl
21:03  0:20      \_ /usr/bin/ibus-daemon
--daemonize --xim
vdsq3226 4089  0.0  0.0   36944   3208 ?      Sl
21:03  0:00      |  \_ /usr/lib/ibus/ibus-dconf
vdsq3226 4090  0.0  0.2 185064  11520 ?      Sl
21:03  0:02      |  \_ /usr/lib/ibus/ibus-ui-gtk3
vdsq3226 4125  0.0  0.0   27580   3024 ?      Sl
21:03  0:05      |  \_ /usr/lib/ibus/ibus-engine-
simple
vdsq3226 4025  0.0  0.3 157460  15704 ?      Ssl
21:03  0:01      \_ /usr/lib/gnome-settings-daemon
/gnome-settings-daemon
vdsq3226 4105  0.0  0.0    3764   792 ?      S
21:03  0:05      |  \_ syndaemon -i 1.0 -t -K -R
vdsq3226 4028  0.0  0.1 65280   5920 ?      Ssl
21:03  0:00      \_ /usr/lib/i386-linux-gnu/hud
/hud-service
vdsq3226 4032  0.0  0.0  44520   3036 ?      Ssl
21:03  0:00      \_ /usr/lib/at-spi2-core/at-spi-
bus-launcher --launch-immediately
vdsq3226 4039  0.0  0.0   3940   1808 ?      S
21:03  0:00      |  \_ /bin/dbus-daemon --config-
```

```
file=/etc/at-spi2/accessibility.conf --nofork --print-
address 3
vdsq3226 4033 0.0 0.2 91756 10068 ? Ssl
21:03 0:00 | \ gnome-session --session=ubuntu
vdsq3226 4179 1.3 1.5 478056 62164 ? Sl
21:03 1:47 | \ compiz
vdsq3226 4389 0.0 0.0 2272 552 ? Ss
21:03 0:00 | | \ /bin/sh -c /usr/bin
/gtk-window-decorator
vdsq3226 4390 0.0 0.2 45380 11656 ? Sl
21:03 0:01 | | \ /usr/bin/gtk-
window-decorator
vdsq3226 4282 0.0 1.0 336488 43444 ? Sl
21:03 0:05 | \ nautilus -n
vdsq3226 4477 0.0 0.2 30012 10816 ? Sl
21:03 0:00 | | \ /usr/bin/python
/usr/lib/python2.7/dist-packages/rabbitvcs/services
/checkerservice.py
vdsq3226 4285 0.0 0.3 321788 16024 ? Sl
21:03 0:01 | \ nm-applet
vdsq3226 4286 0.0 0.2 52112 8376 ? Sl
21:03 0:00 | \ /usr/lib/gnome-settings-
daemon/gnome-fallback-mount-helper
vdsq3226 4287 0.0 0.2 42984 8324 ? Sl
21:03 0:00 | \ /usr/lib/polkit-1-gnome
/polkit-gnome-authentication-agent-1
vdsq3226 4291 0.3 1.3 891684 54788 ? Sl
21:03 0:28 | \ java -Xmx512M
-Dsun.net.inetaddr.ttl=60 -cp /usr/share/davmail
/davmail.jar:/usr/share/java/swt.jar::/usr/share/davmail
/lib/activation-1.1.1.jar:/usr/share/davmail
/lib/commons-codec-1.3.jar:/usr/share/davmail
/lib/commons-collections-3.1.jar:/usr/share/davmail
/lib/commons-httpclient-3.1.jar:/usr/share/davmail
/lib/commons-logging-1.0.4.jar:/usr/share/davmail
/lib/htmlcleaner-2.2.jar:/usr/share/davmail
/lib/jackrabbit-webdav-2.4.3.jar:/usr/share/davmail
/lib/jcharset-1.3.jar:/usr/share/davmail/lib/jcifs-
1.3.14.jar:/usr/share/davmail/lib/jdom-1.0.jar:
/usr/share/davmail/lib/junit-3.8.1.jar:/usr/share
/davmail/lib/log4j-1.2.16.jar:/usr/share/davmail
/lib/mail-1.4.3.jar:/usr/share/davmail/lib/slf4j-
```

```
api-1.3.1.jar:/usr/share/davmail/lib/slf4j-
log4j12-1.3.1.jar:/usr/share/davmail/lib/stax-
api-1.0.1.jar:/usr/share/davmail/lib/stax2-
api-3.1.1.jar:/usr/share/davmail/lib/woodstox-core-
asl-4.1.2.jar:/usr/share/davmail/lib/xercesImpl-
2.8.1.jar davmail.DavGateway
vdsq3226 4292 0.0 0.5 71956 21016 ? S
21:03 0:00 | \_ /usr/bin/python /usr/bin
/gquake
vdsq3226 4365 0.0 0.0 2440 716 ? S
21:03 0:00 | | \_ gnome-pty-helper
vdsq3226 4366 0.0 0.0 7056 3100 pts/5 Ss+
21:03 0:00 | | \_ /bin/bash
vdsq3226 4501 0.0 0.2 78324 9432 ? S
21:03 0:00 | \_ telepathy-indicator
vdsq3226 4511 0.0 0.1 93988 7784 ? S
21:03 0:00 | \_ zeitgeist-datahub
vdsq3226 4544 0.0 0.4 136832 17780 ? S
21:03 0:00 | \_ /usr/lib/evolution
/3.8/evolution-alarm-notify
vdsq3226 4572 0.0 0.2 62220 9936 ? S
21:04 0:00 | \_ update-notifier
vdsq3226 4710 0.0 0.0 48148 3576 ? S
21:05 0:00 | \_ /usr/lib/i386-linux-
gnu/deja-dup/deja-dup-monitor
vdsq3226 4038 0.0 0.3 188360 15876 ? S
21:03 0:05 | \_ /usr/lib/unity/unity-panel-
service
vdsq3226 4046 0.0 0.0 4972 632 ? S
21:03 0:00 | \_ upstart-dbus-bridge --daemon
--session --user --bus-name session
vdsq3226 4047 0.0 0.0 4972 624 ? S
21:03 0:00 | \_ upstart-dbus-bridge --daemon
--system --user --bus-name system
vdsq3226 4048 0.0 0.0 5252 692 ? S
21:03 0:00 | \_ upstart-file-bridge --daemon
--user
vdsq3226 4051 0.0 0.0 27840 2912 ? S
21:03 0:00 | \_ /usr/lib/gvfs/gvfsd
vdsq3226 4053 0.0 0.0 17288 3036 ? S
21:03 0:00 | \_ /usr/lib/at-spi2-core/at-spi2-
registryd --use-gnome-session
```

```
vdsq3226 4061 0.0 0.0 43748 2740 ? Sl
21:03 0:00          \_ /usr/lib/gvfs//gvfsd-fuse -f
/run/user/1000/gvfs
vdsq3226 4092 0.0 0.1 50252 6672 ? Sl
21:03 0:00          \_ /usr/lib/ibus/ibus-x11 --kill-
daemon
vdsq3226 4101 0.0 0.0 24700 2712 ? Sl
21:03 0:00          \_ /usr/lib/dconf/dconf-service
vdsq3226 4112 0.3 0.1 100252 5712 ? S<l
21:03 0:23          \_ /usr/bin/pulseaudio --start
--log-target=syslog
vdsq3226 4120 0.0 0.2 194412 11296 ? Sl
21:03 0:02          \_ /usr/lib/i386-linux-gnu/bamf
/bamfdaemon
vdsq3226 4181 0.0 0.1 56540 4484 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-application-service
vdsq3226 4183 0.0 0.2 64448 9984 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-printers-service
vdsq3226 4187 0.0 0.0 106452 4004 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-sound/indicator-sound-service
vdsq3226 4190 0.0 0.0 46052 3148 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-messages/indicator-messages-service
vdsq3226 4192 0.0 0.0 36520 2832 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-bluetooth/indicator-bluetooth-service
vdsq3226 4198 0.0 0.0 57308 3912 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-sync/indicator-sync-service
vdsq3226 4199 0.0 0.1 93732 6136 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-datetime-service
vdsq3226 4200 0.0 0.0 46232 3504 ? Sl
21:03 0:01          \_ /usr/lib/i386-linux-
gnu/indicator-power/indicator-power-service
vdsq3226 4201 0.0 0.2 187976 10788 ? Sl
21:03 0:00          \_ /usr/lib/i386-linux-
gnu/indicator-keyboard-service --use-gtk --use-bamf
vdsq3226 4204 0.0 0.0 65968 3540 ? Sl
```

```
21:03  0:00          \_ /usr/lib/i386-linux-
gnu/indicator-session/indicator-session-service
vdsq3226 4229  0.0  0.3 177828 14028 ?           Sl
21:03  0:00          \_ /usr/lib/i386-linux-gnu/notify-
osd
vdsq3226 4233  0.0  0.2 52848  9272 ?           Sl
21:03  0:00          \_ /usr/bin/gnome-screensaver
--no-daemon
vdsq3226 4247  0.0  0.2 92024  8348 ?           Sl
21:03  0:00          \_ /usr/lib/evolution/evolution-
source-registry
vdsq3226 4273  0.0  0.7 131576 30628 ?           Sl
21:03  0:00          \_ /usr/lib/evolution/evolution-
calendar-factory
vdsq3226 4303  0.0  0.1 38396  4512 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfs-udisks2-
volume-monitor
vdsq3226 4307  0.0  0.0 10120   3324 ?           S
21:03  0:00          \_ /usr/lib/i386-linux-gnu/gconf
/gconfd-2
vdsq3226 4335  0.0  0.0 26712   2672 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfs-mtp-volume-
monitor
vdsq3226 4339  0.0  0.0 39316   2836 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfs-afc-volume-
monitor
vdsq3226 4344  0.0  0.0 27944   2920 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfs-gphoto2-
volume-monitor
vdsq3226 4384  0.0  0.0 46784   3468 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfsd-trash
--spawner :1.3 /org/gtk/gvfs/exec_spaw/0
vdsq3226 4482  0.0  0.0 37064   2780 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfsd-burn
--spawner :1.3 /org/gtk/gvfs/exec_spaw/1
vdsq3226 4498  0.0  0.0 18488   3356 ?           Sl
21:03  0:00          \_ /usr/lib/gvfs/gvfsd-metadata
vdsq3226 4519  0.0  0.1 44968   4060 ?           Sl
21:03  0:00          \_ /usr/bin/zeitgeist-daemon
vdsq3226 4525  0.0  0.1 52200   7960 ?           Sl
21:03  0:00          \_ /usr/lib/i386-linux-
gnu/zeitgeist-fts
```

```
vdsq3226 4542 0.0 0.0 4268 288 ? S
21:03 0:00 | \_ /bin/cat
vdsq3226 4596 13.6 16.3 1397240 657680 ? Sl
21:04 17:37 \_ /usr/lib/firefox/firefox
vdsq3226 5412 3.8 0.8 204376 36204 ? Sl
22:13 2:19 | \_ /usr/lib/firefox/plugin-
container /usr/lib/flashplugin-installer
/libflashplayer.so -greomni /usr/lib/firefox/omni.ja
-appomni /usr/lib/firefox/browser/omni.ja -appdir
/usr/lib/firefox/browser 4596 true plugin
vdsq3226 4620 0.0 0.0 34680 2428 ? Sl
21:04 0:00 \_ /usr/lib/libunity-webapps
/unity-webapps-service
vdsq3226 5833 3.3 0.5 216024 20176 ? Sl
23:06 0:15 \_ gnome-terminal
vdsq3226 5842 0.0 0.0 2440 748 ? S
23:06 0:00 \_ gnome-pty-helper
vdsq3226 5843 0.0 0.0 7304 3568 pts/2 Ss
23:06 0:00 \_ bash
vdsq3226 6191 0.3 0.0 5600 1680 pts/2 S+
23:09 0:00 | \_ /bin/bash ./mk_mirror-
v2.sh tmp/
vdsq3226 14558 0.0 0.0 5600 872 pts/2 S+
23:13 0:00 | \_ /bin/bash
./mk_mirror-v2.sh tmp/
vdsq3226 14559 0.0 0.5 32368 23444 pts/2 R+
23:13 0:00 | \_ apt-get
--print-uris download libfffi6:i386
vdsq3226 14560 0.0 0.0 4264 552 pts/2 S+
23:13 0:00 | \_ cut -d -f 1
vdsq3226 14561 0.0 0.0 4272 292 pts/2 S+
23:13 0:00 | \_ tr -d \
vdsq3226 6456 0.0 0.0 7092 3316 pts/6 Ss
23:09 0:00 \_ bash
vdsq3226 12551 0.0 0.0 4268 292 pts/6 S
23:12 0:00 | \_ cat /tmp/f
vdsq3226 12552 0.0 0.0 2272 556 pts/6 S+
23:12 0:00 | \_ /bin/sh -i
vdsq3226 12553 0.0 0.0 2608 328 pts/6 S
23:12 0:00 | \_ nc -l 127.0.0.1 1234
vdsq3226 10855 0.0 0.0 7280 3536 pts/7 Ss
23:12 0:00 \_ bash
```

```
vdsq3226 14565 0.0 0.0 5576 1252 pts/7 R+
23:13 0:00 | \_ ps aux --forest
vdsq3226 12795 0.1 0.0 7056 3276 pts/9 Ss
23:13 0:00 \_ bash
vdsq3226 13223 0.0 0.0 2660 732 pts/9 S+
23:13 0:00 \_ nc localhost 1234
root 1754 0.0 0.0 2740 120 ? Ss
21:02 0:00 /usr/sbin/in.tftpd --listen --user tftp
--address [::]:69 --secure /var/lib/tftpboot
root 1766 0.0 0.0 6696 2244 ? Ss
21:02 0:00 /sbin/wpa_supplicant -B -P
/run/sendsigs.omit.d/wpasupplicant.pid -u -s -0 /var/run
/wpa_supplicant
proxy 1783 0.0 0.3 44980 15968 ? Ss
21:02 0:02 /usr/sbin/squid3 -N -YC -f /etc/squid3
/squid.conf
proxy 2616 0.0 0.0 3520 872 ? Ss
21:02 0:00 \_ (logfile-daemon) /var/log/squid3
/access.log
proxy 2617 0.0 0.0 3636 1076 ? Ss
21:02 0:00 \_ (pinger)
root 1789 0.0 0.0 3964 712 ? Ss
21:02 0:00 /usr/sbin/irqbalance
mysql 1790 0.0 0.9 319316 37920 ? Ssl
21:02 0:07 /usr/sbin/mysqld
127 1829 0.0 0.0 3520 956 ? S
21:02 0:00 dnsmasq -u lxc-dnsmasq --strict-order
--bind-interfaces --pid-file=/var/run/lxc/dnsmasq.pid
--conf-file= --listen-address 10.0.3.1 --dhcp-range
10.0.3.2,10.0.3.254 --dhcp-lease-max=253 --dhcp-no-
override --except-interface=lo --interface=lxcbr0
--dhcp-leasefile=/var/lib/misc/dnsmasq.lxcbr0.leases
--dhcp-authoritative
root 1853 0.0 0.0 15572 892 ? Ss
21:02 0:01 tgtd
root 1855 0.0 0.0 15568 604 ? S
21:02 0:00 \_ tgtd
root 1857 0.0 0.3 138876 12300 ? Sl
21:02 0:00 /usr/sbin/libvirtd -d
postgres 1885 0.0 0.1 48840 7752 ? S
21:02 0:00 /usr/lib/postgresql/9.1/bin/postgres -D
/var/lib/postgresql/9.1/main -c config_file=/etc
```

```
/postgresql/9.1/main/postgresql.conf
postgres 2018 0.0 0.0 48840 1580 ? Ss
21:02 0:01 \_ postgres: writer process
postgres 2019 0.0 0.0 48840 1340 ? Ss
21:02 0:01 \_ postgres: wal writer process
postgres 2020 0.0 0.0 49256 2392 ? Ss
21:02 0:00 \_ postgres: autovacuum launcher process
postgres 2021 0.0 0.0 19072 1392 ? Ss
21:02 0:00 \_ postgres: stats collector process
root 1942 0.0 0.0 35636 3544 ? Sl
21:02 0:00 /usr/lib/accountsservice/accounts-daemon
root 2211 0.0 0.1 38016 4476 ? Sl
21:02 0:02 /usr/lib/upower/upowerd
122 2266 0.0 0.0 3520 964 ? S
21:02 0:00 /usr/sbin/dnsmasq --conf-file=/var
/lib/libvirt/dnsmasq/default.conf
root 2561 0.0 0.0 19112 3600 ? Ss
21:02 0:00 /usr/sbin/winbindd -F
root 2887 0.0 0.0 19112 1580 ? S
21:02 0:00 \_ /usr/sbin/winbindd -F
rtkit 3068 0.0 0.0 21376 1248 ? SNl
21:02 0:00 /usr/lib/rtkit/rtkit-daemon
root 3078 0.0 0.0 26360 3068 ? Sl
21:02 0:00 /usr/sbin/console-kit-daemon --no-daemon
root 3205 0.0 0.0 33428 572 ? Ssl
21:02 0:00 /usr/lib/vmware/bin/vmware-vmblock-fuse -o
subtype=vmware-vmblock,default_permissions,allow_other
/var/run/vmblock-fuse
root 3238 0.0 0.0 13448 508 ? Ss
21:02 0:00 /usr/sbin/vmware-authdlauncher
clamav 3509 0.0 5.2 244600 210956 ? Ssl
21:02 0:05 /usr/sbin/clamd
clamav 3625 0.0 0.0 14416 1864 ? Ss
21:02 0:07 /usr/bin/freshclam -d --quiet
privoxy 3640 0.0 0.0 3432 1300 ? Ss
21:02 0:00 /usr/sbin/privoxy --pidfile /var/run
/privoxy.pid --user privoxy /etc/privoxy/config
root 3721 0.0 0.5 28636 23812 ? Ss
21:02 0:00 /usr/bin/ruby /usr/bin/puppet agent
root 3746 0.0 0.0 13744 1748 ? Ss
21:02 0:00 /usr/bin/vmware-usbarbitrator
root 3836 0.0 0.0 4668 860 tty1 Ss+
```

```

21:02 0:00 /sbin/getty -8 38400 ttym1
vdsq3226 3898 0.0 0.0 55488 3500 ? Sl
21:03 0:00 /usr/bin/gnome-keyring-daemon --daemonize
--login
root      4317 0.0 0.1 53056 4556 ? Sl
21:03 0:00 /usr/lib/udisks2/udisksd --no-debug

```

## Exemple Netstat

version : 12-10-2014 18:02

netstat -tanpeo

Connexions Internet actives (serveurs et établies)					
Proto	Recv-Q	Send-Q	Adresse locale	Adresse	
distant			User	Inode	
PID/Program name	Etat	Timer			
tcp	0	0	0.0.0.0:3260	0.0.0.0:*	
LISTEN	0		14660	1853/tgtd	off
(0.00/0/0)					
tcp	0	0	0.0.0.0:902	0.0.0.0:*	
LISTEN	0		16144	3238/vmware-authdla	
off (0.00/0/0)					
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	
LISTEN	131		15462	1790/mysqld	off
(0.00/0/0)					
tcp	0	0	192.168.122.1:53	0.0.0.0:*	
LISTEN	0		15663	2266/dnsmasq	off
(0.00/0/0)					
tcp	0	0	127.0.1.1:53	0.0.0.0:*	
LISTEN	0		15583	2137/dnsmasq	off
(0.00/0/0)					
tcp	0	0	10.0.3.1:53	0.0.0.0:*	
LISTEN	0		11970	1829/dnsmasq	off
(0.00/0/0)					
tcp	0	0	127.0.0.1:8118	0.0.0.0:*	
LISTEN	120		17749	3640/privoxy	off
(0.00/0/0)					
tcp	0	0	0.0.0.0:22	0.0.0.0:*	
LISTEN	0		11844	1671/sshd	off
(0.00/0/0)					
tcp	0	0	127.0.0.1:631	0.0.0.0:*	

LISTEN	0 (0.00/0/0)	11700	1138/cupsd	off
tcp	0	0 127.0.0.1:5432	0.0.0.0:*	
LISTEN	124 (0.00/0/0)	14706	1885/postgres	off
tcp	0	0 192.168.1.14:48072		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (39,79/0/0)		
tcp	0	0 192.168.1.14:48039		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (8,65/0/0)		
tcp	0	0 192.168.1.14:48109		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (55,56/0/0)		
tcp	0	0 192.168.1.14:48105		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (54,06/0/0)		
tcp	0	0 192.168.1.14:43609		
173.194.40.181:443		ESTABLISHED 1000		57534
4596/firefox		off (0.00/0/0)		
tcp	0	0 192.168.1.14:48084		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (45,17/0/0)		
tcp	0	0 192.168.1.14:48079		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (43,38/0/0)		
tcp	0	0 192.168.1.14:48112		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (57,12/0/0)		
tcp	0	0 192.168.1.14:48060		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (29,72/0/0)		
tcp	0	0 192.168.1.14:48051		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (25,63/0/0)		
tcp	0	0 192.168.1.14:48052		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (26,05/0/0)		
tcp	0	0 192.168.1.14:48062		
158.255.96.2:80		TIME_WAIT 0		0
-		temps d'attente (30,45/0/0)		
tcp	0	0 192.168.1.14:48118		

158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(59,94/0/0)
tcp 0	0 192.168.1.14:48049	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(24,42/0/0)
tcp 0	0 192.168.1.14:48069	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(39,08/0/0)
tcp 0	0 192.168.1.14:48048	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(23,78/0/0)
tcp 0	0 192.168.1.14:48095	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(49,77/0/0)
tcp 0	0 192.168.1.14:48100	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(51,95/0/0)
tcp 0	0 192.168.1.14:48076	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(41,01/0/0)
tcp 0	0 192.168.1.14:48082	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(44,40/0/0)
tcp 0	0 192.168.1.14:48093	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(49,04/0/0)
tcp 0	0 192.168.1.14:48055	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(27,37/0/0)
tcp 0	0 192.168.1.14:48066	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(37,65/0/0)
tcp 0	0 192.168.1.14:48099	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(51,49/0/0)
tcp 0	0 192.168.1.14:48056	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(27,86/0/0)
tcp 0	0 192.168.1.14:48054	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(26,98/0/0)
tcp 0	0 192.168.1.14:48107	

158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(54,81/0/0)	
tcp 0	0 192.168.1.14:48083		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(44,77/0/0)	
tcp 0	0 127.0.0.1:1234		
127.0.0.1:55642	ESTABLISHED	1000	134435
31628/nc	off	(0.00/0/0)	
tcp 0	0 192.168.1.14:48077		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(41,36/0/0)	
tcp 0	0 192.168.1.14:39064		
173.194.34.41:443	ESTABLISHED	1000	133350
4596/firefox	off	(0.00/0/0)	
tcp 0	0 192.168.1.14:48044		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(21,59/0/0)	
tcp 0	0 192.168.1.14:48080		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(43,71/0/0)	
tcp 0	0 192.168.1.14:48047		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(23,28/0/0)	
tcp 0	0 192.168.1.14:48113		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(58,53/0/0)	
tcp 0	0 192.168.1.14:48078		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(41,76/0/0)	
tcp 0	0 192.168.1.14:48102		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(52,73/0/0)	
tcp 0	0 127.0.0.1:55642		
127.0.0.1:1234	ESTABLISHED	1000	132512
31674/nc	off	(0.00/0/0)	
tcp 0	0 192.168.1.14:48103		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(53,11/0/0)	
tcp 0	0 192.168.1.14:48067		
158.255.96.2:80	TIME_WAIT	0	0
-	temps d'attente	(38,04/0/0)	
tcp 0	0 192.168.1.14:48097		

158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(50,68/0/0)
tcp 0	0 192.168.1.14:48104	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(53,67/0/0)
tcp 0	0 192.168.1.14:48057	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(28,34/0/0)
tcp 0	0 192.168.1.14:48061	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(30,12/0/0)
tcp 0	0 192.168.1.14:48085	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(45,51/0/0)
tcp 0	0 192.168.1.14:48096	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(50,19/0/0)
tcp 0	0 192.168.1.14:48091	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(48,22/0/0)
tcp 0	0 192.168.1.14:48081	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(44,05/0/0)
tcp 0	0 192.168.1.14:48108	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(55,14/0/0)
tcp 0	0 192.168.1.14:48086	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(45,94/0/0)
tcp 0	0 192.168.1.14:48068	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(38,66/0/0)
tcp 0	0 192.168.1.14:48087	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(46,25/0/0)
tcp 0	0 192.168.1.14:48075	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(40,65/0/0)
tcp 0	0 192.168.1.14:48041	
158.255.96.2:80	TIME_WAIT	0
-	temps d'attente	(21,11/0/0)
tcp 45	0 192.168.1.14:46170	

199.16.156.52:443		ESTABLISHED	1000	132773
4596/firefox	off (0.00/0/0)			
tcp 0	0 192.168.1.14:48053	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (26,44/0/0)			
-				
tcp 0	0 192.168.1.14:48090	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (47,29/0/0)			
-				
tcp 0	0 192.168.1.14:48063	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (30,85/0/0)			
-				
tcp 0	0 192.168.1.14:48116	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (59,28/0/0)			
-				
tcp 0	0 192.168.1.14:48110	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (56,36/0/0)			
-				
tcp 0	0 192.168.1.14:48101	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (52,32/0/0)			
-				
tcp 0	0 192.168.1.14:48092	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (48,64/0/0)			
-				
tcp 0	0 192.168.1.14:48111	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (56,69/0/0)			
-				
tcp 0	0 192.168.1.14:48098	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (51,09/0/0)			
-				
tcp 0	0 192.168.1.14:48106	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (54,42/0/0)			
-				
tcp 0	0 192.168.1.14:48094	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (49,40/0/0)			
-				
tcp 0	0 192.168.1.14:48059	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (28,98/0/0)			
-				
tcp 0	0 192.168.1.14:48065	TIME_WAIT	0	0
158.255.96.2:80	temps d'attente (36,83/0/0)			
-				
tcp 0	0 192.168.1.14:48117	TIME_WAIT	0	0

		TIME_WAIT	0	
-		temps d'attente	(59,58/0/0)	
tcp	0	0 192.168.1.14:48115		
158.255.96.2:80		TIME_WAIT	0	0
-		temps d'attente	(58,92/0/0)	
tcp	0	0 192.168.1.14:48089		
158.255.96.2:80		TIME_WAIT	0	0
-		temps d'attente	(46,95/0/0)	
tcp	0	0 192.168.1.14:48070		
158.255.96.2:80		TIME_WAIT	0	0
-		temps d'attente	(39,42/0/0)	
tcp	0	0 192.168.1.14:48064		
158.255.96.2:80		TIME_WAIT	0	0
-		temps d'attente	(31,29/0/0)	
tcp6	0	0 ::::3260		::::*
LISTEN	0	14661	1853/tgtd	off
(0.00/0/0)				
tcp6	0	0 127.0.0.1:1025		::::*
LISTEN	1000	21515	4291/java	off
(0.00/0/0)				
tcp6	0	0 127.0.0.1:1389		::::*
LISTEN	1000	21519	4291/java	off
(0.00/0/0)				
tcp6	0	0 fe80::54bc:98ff:fec4:53		::::*
LISTEN	127	13756	1829/dnsmasq	off
(0.00/0/0)				
tcp6	0	0 ::::4949		::::*
LISTEN	0	12906	1043/perl	off
(0.00/0/0)				
tcp6	0	0 127.0.0.1:1110		::::*
LISTEN	1000	21516	4291/java	off
(0.00/0/0)				
tcp6	0	0 ::::22		::::*
LISTEN	0	11846	1671/sshd	off
(0.00/0/0)				
tcp6	0	0 127.0.0.1:1143		::::*
LISTEN	1000	21517	4291/java	off
(0.00/0/0)				
tcp6	0	0 ::1:631		::::*
LISTEN	0	11699	1138/cupsd	off
(0.00/0/0)				
tcp6	0	0 127.0.0.1:1080		::::*

LISTEN	1000	21518	4291/java	off
(0.00/0/0)				
tcp6	0	0 ::::3128	::::*	
LISTEN	0	15160	1783/squid3	off
(0.00/0/0)				
tcp6	1	0 127.0.0.1:57344		
127.0.0.1:3128		CLOSE_WAIT	1000	21524
4291/java		off	(0.00/0/0)	

## Exemple avec lsof

version : 12-10-2014 18:02

lsof | grep vdsq3226 | grep "/tmp"

gpg-agent	3983	vdsq3226	5u	unix
0x00000000	0t0	20219	/tmp/gpg-iy7XiB/S.gpg-agent	
dbus-daem	3987	vdsq3226	4u	unix
0x00000000	0t0	16968	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	8u	unix
0x00000000	0t0	20224	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	9u	unix
0x00000000	0t0	18718	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	10u	unix
0x00000000	0t0	20231	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	11u	unix
0x00000000	0t0	20242	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	12u	unix
0x00000000	0t0	20238	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	13u	unix
0x00000000	0t0	20244	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	14u	unix
0x00000000	0t0	17039	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	15u	unix
0x00000000	0t0	20293	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	16u	unix
0x00000000	0t0	18793	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	17u	unix
0x00000000	0t0	17060	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	18u	unix
0x00000000	0t0	17059	@/tmp/dbus-zuJUndsZ7H	
dbus-daem	3987	vdsq3226	19u	unix

0x00000000	0t0	18812	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	20u unix
0x00000000	0t0	20469	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	21u unix
0x00000000	0t0	20391	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	22u unix
0x00000000	0t0	17263	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	23u unix
0x00000000	0t0	17105	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	24u unix
0x00000000	0t0	20392	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	25u unix
0x00000000	0t0	18897	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	26u unix
0x00000000	0t0	18898	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	27u unix
0x00000000	0t0	18233	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	28u unix
0x00000000	0t0	18976	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	29u unix
0x00000000	0t0	20498	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	30u unix
0x00000000	0t0	18979	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	31u unix
0x00000000	0t0	18402	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	32u unix
0x00000000	0t0	18366	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	33u unix
0x00000000	0t0	17277	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	34u unix
0x00000000	0t0	18337	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	35u unix
0x00000000	0t0	18367	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	36u unix
0x00000000	0t0	18970	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	37u unix
0x00000000	0t0	17253	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	38u unix
0x00000000	0t0	18951	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	39u unix
0x00000000	0t0	17254	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	40u unix

0x00000000	0t0	18353	@/tmp/dbus-zuJUndsZ7H vdsq3226 41u unix
dbus-daem	3987		
0x00000000	0t0	18952	@/tmp/dbus-zuJUndsZ7H vdsq3226 42u unix
dbus-daem	3987		
0x00000000	0t0	21512	@/tmp/dbus-zuJUndsZ7H vdsq3226 43u unix
dbus-daem	3987		
0x00000000	0t0	18356	@/tmp/dbus-zuJUndsZ7H vdsq3226 44u unix
dbus-daem	3987		
0x00000000	0t0	18953	@/tmp/dbus-zuJUndsZ7H vdsq3226 45u unix
dbus-daem	3987		
0x00000000	0t0	19042	@/tmp/dbus-zuJUndsZ7H vdsq3226 46u unix
dbus-daem	3987		
0x00000000	0t0	18294	@/tmp/dbus-zuJUndsZ7H vdsq3226 47u unix
dbus-daem	3987		
0x00000000	0t0	19081	@/tmp/dbus-zuJUndsZ7H vdsq3226 48u unix
dbus-daem	3987		
0x00000000	0t0	20486	@/tmp/dbus-zuJUndsZ7H vdsq3226 49u unix
dbus-daem	3987		
0x00000000	0t0	20487	@/tmp/dbus-zuJUndsZ7H vdsq3226 50u unix
dbus-daem	3987		
0x00000000	0t0	20488	@/tmp/dbus-zuJUndsZ7H vdsq3226 51u unix
dbus-daem	3987		
0x00000000	0t0	20490	@/tmp/dbus-zuJUndsZ7H vdsq3226 52u unix
dbus-daem	3987		
0x00000000	0t0	19088	@/tmp/dbus-zuJUndsZ7H vdsq3226 53u unix
dbus-daem	3987		
0x00000000	0t0	18429	@/tmp/dbus-zuJUndsZ7H vdsq3226 54u unix
dbus-daem	3987		
0x00000000	0t0	17289	@/tmp/dbus-zuJUndsZ7H vdsq3226 55u unix
dbus-daem	3987		
0x00000000	0t0	19070	@/tmp/dbus-zuJUndsZ7H vdsq3226 56u unix
dbus-daem	3987		
0x00000000	0t0	17319	@/tmp/dbus-zuJUndsZ7H vdsq3226 57u unix
dbus-daem	3987		
0x00000000	0t0	19092	@/tmp/dbus-zuJUndsZ7H vdsq3226 58u unix
dbus-daem	3987		
0x00000000	0t0	19095	@/tmp/dbus-zuJUndsZ7H vdsq3226 59u unix
dbus-daem	3987		
0x00000000	0t0	20693	@/tmp/dbus-zuJUndsZ7H vdsq3226 60u unix
dbus-daem	3987		
0x00000000	0t0	20695	@/tmp/dbus-zuJUndsZ7H vdsq3226 61u unix
dbus-daem	3987		

0x00000000	0t0	19096	@/tmp/dbus-zuJUndsZ7H vdsq3226 62u unix
dbus-daem	3987		
0x00000000	0t0	17334	@/tmp/dbus-zuJUndsZ7H vdsq3226 63u unix
dbus-daem	3987		
0x00000000	0t0	21547	@/tmp/dbus-zuJUndsZ7H vdsq3226 64u unix
dbus-daem	3987		
0x00000000	0t0	20729	@/tmp/dbus-zuJUndsZ7H vdsq3226 65u unix
dbus-daem	3987		
0x00000000	0t0	21752	@/tmp/dbus-zuJUndsZ7H vdsq3226 66u unix
dbus-daem	3987		
0x00000000	0t0	20789	@/tmp/dbus-zuJUndsZ7H vdsq3226 67u unix
dbus-daem	3987		
0x00000000	0t0	21741	@/tmp/dbus-zuJUndsZ7H vdsq3226 68u unix
dbus-daem	3987		
0x00000000	0t0	19136	@/tmp/dbus-zuJUndsZ7H vdsq3226 69u unix
dbus-daem	3987		
0x00000000	0t0	19194	@/tmp/dbus-zuJUndsZ7H vdsq3226 70u unix
dbus-daem	3987		
0x00000000	0t0	22622	@/tmp/dbus-zuJUndsZ7H vdsq3226 71u unix
dbus-daem	3987		
0x00000000	0t0	19201	@/tmp/dbus-zuJUndsZ7H vdsq3226 72u unix
dbus-daem	3987		
0x00000000	0t0	22701	@/tmp/dbus-zuJUndsZ7H vdsq3226 73u unix
dbus-daem	3987		
0x00000000	0t0	19248	@/tmp/dbus-zuJUndsZ7H vdsq3226 74u unix
dbus-daem	3987		
0x00000000	0t0	22672	@/tmp/dbus-zuJUndsZ7H vdsq3226 75u unix
dbus-daem	3987		
0x00000000	0t0	22718	@/tmp/dbus-zuJUndsZ7H vdsq3226 76u unix
dbus-daem	3987		
0x00000000	0t0	22758	@/tmp/dbus-zuJUndsZ7H vdsq3226 77u unix
dbus-daem	3987		
0x00000000	0t0	22226	@/tmp/dbus-zuJUndsZ7H vdsq3226 78u unix
dbus-daem	3987		
0x00000000	0t0	21037	@/tmp/dbus-zuJUndsZ7H vdsq3226 79u unix
dbus-daem	3987		
0x00000000	0t0	21033	@/tmp/dbus-zuJUndsZ7H vdsq3226 80u unix
dbus-daem	3987		
0x00000000	0t0	23673	@/tmp/dbus-zuJUndsZ7H vdsq3226 81u unix
dbus-daem	3987		
0x00000000	0t0	41334	@/tmp/dbus-zuJUndsZ7H vdsq3226 82u unix
dbus-daem	3987		

0x00000000	0t0	55567	@/tmp/dbus-zuJUndsZ7H
dbus-daem	3987	vdsq3226	83u unix
0x00000000	0t0	53234	@/tmp/dbus-zuJUndsZ7H
ibus-daem	4011	vdsq3226	9u unix
0x00000000	0t0	20248	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	11u unix
0x00000000	0t0	18789	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	13u unix
0x00000000	0t0	17062	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	15u unix
0x00000000	0t0	20363	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	17u unix
0x00000000	0t0	17131	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	19u unix
0x00000000	0t0	17264	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	21u unix
0x00000000	0t0	19113	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	23u unix
0x00000000	0t0	22632	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	25u unix
0x00000000	0t0	22759	@/tmp/dbus-WoUlXseq
ibus-daem	4011	vdsq3226	27u unix
0x00000000	0t0	55569	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 9u unix
0x00000000	0t0	20248	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 11u unix
0x00000000	0t0	18789	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 13u unix
0x00000000	0t0	17062	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 15u unix
0x00000000	0t0	20363	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 17u unix
0x00000000	0t0	17131	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 19u unix
0x00000000	0t0	17264	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 21u unix
0x00000000	0t0	19113	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 23u unix
0x00000000	0t0	22632	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 25u unix
0x00000000	0t0	22759	@/tmp/dbus-WoUlXseq
gdbus	4011	4049	vdsq3226 27u unix

0x00000000	0t0	55569	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 9u unix
0x00000000	0t0	20248	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 11u unix
0x00000000	0t0	18789	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 13u unix
0x00000000	0t0	17062	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 15u unix
0x00000000	0t0	20363	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 17u unix
0x00000000	0t0	17131	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 19u unix
0x00000000	0t0	17264	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 21u unix
0x00000000	0t0	19113	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 23u unix
0x00000000	0t0	22632	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 25u unix
0x00000000	0t0	22759	@/tmp/dbus-WoUlXseq
gmain	4011	4063	vdsq3226 27u unix
0x00000000	0t0	55569	@/tmp/dbus-WoUlXseq
gnome-ses	4033		vdsq3226 15u unix
0x00000000	0t0	17129	@/tmp/.ICE-unix/4033
gnome-ses	4033		vdsq3226 16u unix
0x00000000	0t0	17130	/tmp/.ICE-unix/4033
gnome-ses	4033		vdsq3226 18u unix
0x00000000	0t0	20467	@/tmp/.ICE-unix/4033
gnome-ses	4033		vdsq3226 19u unix
0x00000000	0t0	18981	@/tmp/.ICE-unix/4033
gnome-ses	4033		vdsq3226 21u unix
0x00000000	0t0	19372	@/tmp/.ICE-unix/4033
gnome-ses	4033		vdsq3226 22u unix
0x00000000	0t0	53233	@/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 15u unix
0x00000000	0t0	17129	@/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 16u unix
0x00000000	0t0	17130	/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 18u unix
0x00000000	0t0	20467	@/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 19u unix
0x00000000	0t0	18981	@/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 21u unix

0x00000000	0t0	19372	@/tmp/.ICE-unix/4033
dconf	4033	4133	vdsq3226 22u unix
0x00000000	0t0	53233	@/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 15u unix
0x00000000	0t0	17129	@/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 16u unix
0x00000000	0t0	17130	/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 18u unix
0x00000000	0t0	20467	@/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 19u unix
0x00000000	0t0	18981	@/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 21u unix
0x00000000	0t0	19372	@/tmp/.ICE-unix/4033
gdbus	4033	4134	vdsq3226 22u unix
0x00000000	0t0	53233	@/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 15u unix
0x00000000	0t0	17129	@/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 16u unix
0x00000000	0t0	17130	/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 18u unix
0x00000000	0t0	20467	@/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 19u unix
0x00000000	0t0	18981	@/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 21u unix
0x00000000	0t0	19372	@/tmp/.ICE-unix/4033
gmain	4033	4135	vdsq3226 22u unix
0x00000000	0t0	53233	@/tmp/.ICE-unix/4033
dbus-daem	4039		vdsq3226 5u unix
0x00000000	0t0	17019	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 8u unix
0x00000000	0t0	17025	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 9u unix
0x00000000	0t0	20292	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 10u unix
0x00000000	0t0	20239	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 11u unix
0x00000000	0t0	17122	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 12u unix
0x00000000	0t0	18185	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 13u unix
0x00000000	0t0	18937	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039		vdsq3226 14u unix

0x00000000	0t0	18945	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	15u unix
0x00000000	0t0	18947	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	16u unix
0x00000000	0t0	18961	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	17u unix
0x00000000	0t0	18962	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	18u unix
0x00000000	0t0	19033	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	19u unix
0x00000000	0t0	19034	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	20u unix
0x00000000	0t0	20625	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	21u unix
0x00000000	0t0	20690	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	22u unix
0x00000000	0t0	19107	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	23u unix
0x00000000	0t0	22700	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	24u unix
0x00000000	0t0	20818	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	25u unix
0x00000000	0t0	19351	@/tmp/dbus-YbTUpCowtN
dbus-daem	4039	vdsq3226	26u unix
0x00000000	0t0	54212	@/tmp/dbus-YbTUpCowtN
java	4291	vdsq3226	mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4310	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4311	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4312	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4313	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4314	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4321	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4323	vdsq3226 mem REG
252,1	32768	7340135	/tmp/hsperfdata vdsq3226/4291
java	4291	4324	vdsq3226 mem REG

252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4325	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4326	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4327	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4328	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4329	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4330	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4345	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4346	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4347	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
dconf	4291	4352	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
dbus	4291	4353	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4356	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4357	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4358	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4359	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4360	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
java	4291	4361	vdsq3226	mem	REG
252,1	32768	7340135	/tmp/hsperfdata_vdsq3226/4291		
firefox	4596		vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
firefox	4596		vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Gecko IOT	4596	4602	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		

Gecko_IOT	4596	4602	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Socket	4596	4603	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Socket	4596	4603	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
JS	4596	4604	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
JS	4596	4604	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
JS	4596	4605	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
JS	4596	4605	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Hang	4596	4606	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Hang	4596	4606	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
dbus	4596	4607	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
dbus	4596	4607	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
gmain	4596	4608	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
gmain	4596	4608	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mpegaudio	4596	4610	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mpegaudio	4596	4610	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Analysis	4596	4612	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Analysis	4596	4612	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		

(deleted)  
Analysis 4596 4613 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
Analysis 4596 4613 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
Analysis 4596 4614 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
Analysis 4596 4614 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
Analysis 4596 4615 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
Analysis 4596 4615 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
Timer 4596 4616 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
Timer 4596 4616 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
DOM 4596 4618 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
DOM 4596 4618 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
DOM 4596 4631 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
DOM 4596 4631 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
Cache 4596 4632 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
Cache 4596 4632 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
HTML5 4596 4633 vdsq3226 DEL REG  
252,1 7342703 /tmp/orcexec.zkjh35  
HTML5 4596 4633 vdsq3226 65u REG  
252,1 32768 7340824 /tmp/mozilla-temp-1899493789  
(deleted)  
dconf 4596 4657 vdsq3226 DEL REG

252,1		7342703	/tmp/orcexec.zkjh35		
dconf	4596	4657	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	4661	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4661	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	4662	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4662	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	4663	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4663	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Cert	4596	4665	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Cert	4596	4665	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Proxy	4596	4666	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Proxy	4596	4666	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
localStor	4596	4667	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
localStor	4596	4667	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	4670	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4670	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
Image	4596	4673	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Image	4596	4673	vdsq3226	65u	REG

252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
URL	4596	4674	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
URL	4596	4674	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
DOM	4596	4683	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
DOM	4596	4683	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
mozStorage	4596	4687	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4687	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
MediaManager	4596	4689	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
MediaManager	4596	4689	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
firefox	4596	4702	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
firefox	4596	4702	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
Media	4596	4703	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
Media	4596	4703	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
queue:sr	4596	4705	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
queue:sr	4596	4705	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		
mozStorage	4596	4706	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4706	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789 (deleted)		

mozStorage	4596	4749	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4749	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	4750	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	4750	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
firefox	4596	4756	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
firefox	4596	4756	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
threaded-	4596	5176	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
threaded-	4596	5176	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
mozStorage	4596	5428	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
mozStorage	4596	5428	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
DNS	4596	10293	vdsq3226	DEL	REG
252,1		7342703	/tmp/orcexec.zkjh35		
DNS	4596	10293	vdsq3226	65u	REG
252,1	32768	7340824	/tmp/mozilla-temp-1899493789		
(deleted)					
gnome-ter	5833		vdsq3226	21u	REG
252,1	20780	7342706	/tmp/vtELMXD9W	(deleted)	
gnome-ter	5833		vdsq3226	22u	REG
252,1	2504	7342710	/tmp/vteMGXD9W	(deleted)	
gnome-ter	5833		vdsq3226	23u	REG
252,1	0	7346448	/tmp/vteBBXD9W	(deleted)	
gnome-ter	5833		vdsq3226	24u	REG
252,1	458	7346484	/tmp/vteSLYw8W	(deleted)	
gnome-ter	5833		vdsq3226	25u	REG
252,1	24	7346485	/tmp/vte2MYw8W	(deleted)	
gnome-ter	5833		vdsq3226	26u	REG
252,1	8	7346486	/tmp/vteRPYw8W	(deleted)	

gnome-ter	5833		vdsq3226	29u	REG
252,1	34010	7346490	/tmp/vteR0ID9W	(deleted)	
gnome-ter	5833		vdsq3226	30u	REG
252,1	4096	7346494	/tmp/vte1TID9W	(deleted)	
gnome-ter	5833		vdsq3226	31u	REG
252,1	44074	7346495	/tmp/vteDM558W	(deleted)	
gnome-ter	5833		vdsq3226	32u	REG
252,1	3656	7346496	/tmp/vte9U558W	(deleted)	
gnome-ter	5833		vdsq3226	33u	REG
252,1	0	7346497	/tmp/vteTH3U8W	(deleted)	
gnome-ter	5833		vdsq3226	34u	REG
252,1	0	7346498	/tmp/vteQF3U8W	(deleted)	
gnome-ter	5833		vdsq3226	35u	REG
252,1	0	7346499	/tmp/vteRE3U8W	(deleted)	
gnome-ter	5833		vdsq3226	36u	REG
252,1	128	7346500	/tmp/vteMMCX8W	(deleted)	
gnome-ter	5833		vdsq3226	37u	REG
252,1	1526	7346501	/tmp/vte2NCX8W	(deleted)	
gnome-ter	5833		vdsq3226	38u	REG
252,1	248	7346502	/tmp/vteK0CX8W	(deleted)	
gnome-ter	5833		vdsq3226	41u	REG
252,1	2456	7346504	/tmp/vte9S6U8W	(deleted)	
gnome-ter	5833		vdsq3226	42u	REG
252,1	312	7346505	/tmp/vteXU6U8W	(deleted)	
gnome-ter	5833		vdsq3226	43u	REG
252,1	872	7346506	/tmp/vteXH6U8W	(deleted)	
gnome-ter	5833		vdsq3226	44u	REG
252,1	64	7346522	/tmp/vteWZ658W	(deleted)	
gnome-ter	5833		vdsq3226	45u	REG
252,1	218	7346523	/tmp/vteT1658W	(deleted)	
gnome-ter	5833		vdsq3226	46u	REG
252,1	48	7346524	/tmp/vteG4658W	(deleted)	
gnome-ter	5833		vdsq3226	49u	REG
252,1	24371	7346527	/tmp/vteJRJW8W	(deleted)	
gnome-ter	5833		vdsq3226	50u	REG
252,1	2064	7346528	/tmp/vte5LJW8W	(deleted)	
gnome-ter	5833		vdsq3226	51u	REG
252,1	12029	7346529	/tmp/vteVKS88W	(deleted)	
gnome-ter	5833		vdsq3226	52u	REG
252,1	904	7346530	/tmp/vteDNS88W	(deleted)	
gnome-ter	5833		vdsq3226	53u	REG
252,1	56568	7346532	/tmp/vte4WCB9W	(deleted)	

gnome-ter	5833		vdsq3226	54u	REG
252,1	4096	7346533	/tmp/vteIVCB9W	(deleted)	
gnome-ter	5833		vdsq3226	55u	REG
252,1	0	7346534	/tmp/vtePNT28W	(deleted)	
gnome-ter	5833		vdsq3226	56u	REG
252,1	0	7346535	/tmp/vte02I18W	(deleted)	
dconf	5833	5836	vdsq3226	21u	REG
252,1	20780	7342706	/tmp/vteLMXD9W	(deleted)	
dconf	5833	5836	vdsq3226	22u	REG
252,1	2504	7342710	/tmp/vteMGXD9W	(deleted)	
dconf	5833	5836	vdsq3226	23u	REG
252,1	0	7346448	/tmp/vteBBXD9W	(deleted)	
dconf	5833	5836	vdsq3226	24u	REG
252,1	458	7346484	/tmp/vteSLYW8W	(deleted)	
dconf	5833	5836	vdsq3226	25u	REG
252,1	24	7346485	/tmp/vte2MYW8W	(deleted)	
dconf	5833	5836	vdsq3226	26u	REG
252,1	8	7346486	/tmp/vteRPYW8W	(deleted)	
dconf	5833	5836	vdsq3226	29u	REG
252,1	34010	7346490	/tmp/vteROID9W	(deleted)	
dconf	5833	5836	vdsq3226	30u	REG
252,1	4096	7346494	/tmp/vte1TID9W	(deleted)	
dconf	5833	5836	vdsq3226	31u	REG
252,1	44074	7346495	/tmp/vteDM558W	(deleted)	
dconf	5833	5836	vdsq3226	32u	REG
252,1	3656	7346496	/tmp/vte9U558W	(deleted)	
dconf	5833	5836	vdsq3226	33u	REG
252,1	0	7346497	/tmp/vteTH3U8W	(deleted)	
dconf	5833	5836	vdsq3226	34u	REG
252,1	0	7346498	/tmp/vteQF3U8W	(deleted)	
dconf	5833	5836	vdsq3226	35u	REG
252,1	0	7346499	/tmp/vteRE3U8W	(deleted)	
dconf	5833	5836	vdsq3226	36u	REG
252,1	128	7346500	/tmp/vteMMCX8W	(deleted)	
dconf	5833	5836	vdsq3226	37u	REG
252,1	1526	7346501	/tmp/vte2NCX8W	(deleted)	
dconf	5833	5836	vdsq3226	38u	REG
252,1	248	7346502	/tmp/vteK0CX8W	(deleted)	
dconf	5833	5836	vdsq3226	41u	REG
252,1	2456	7346504	/tmp/vte9S6U8W	(deleted)	
dconf	5833	5836	vdsq3226	42u	REG
252,1	312	7346505	/tmp/vteXU6U8W	(deleted)	

dconf	5833	5836	vdsq3226	43u	REG
252,1	872	7346506	/tmp/vteXH6U8W	(deleted)	
dconf	5833	5836	vdsq3226	44u	REG
252,1	64	7346522	/tmp/vteWZ658W	(deleted)	
dconf	5833	5836	vdsq3226	45u	REG
252,1	218	7346523	/tmp/vteT1658W	(deleted)	
dconf	5833	5836	vdsq3226	46u	REG
252,1	48	7346524	/tmp/vteG4658W	(deleted)	
dconf	5833	5836	vdsq3226	49u	REG
252,1	24371	7346527	/tmp/vteJRJW8W	(deleted)	
dconf	5833	5836	vdsq3226	50u	REG
252,1	2064	7346528	/tmp/vte5LJW8W	(deleted)	
dconf	5833	5836	vdsq3226	51u	REG
252,1	12029	7346529	/tmp/vteVKS88W	(deleted)	
dconf	5833	5836	vdsq3226	52u	REG
252,1	904	7346530	/tmp/vteDNS88W	(deleted)	
dconf	5833	5836	vdsq3226	53u	REG
252,1	56568	7346532	/tmp/vte4WCB9W	(deleted)	
dconf	5833	5836	vdsq3226	54u	REG
252,1	4096	7346533	/tmp/vteIVCB9W	(deleted)	
dconf	5833	5836	vdsq3226	55u	REG
252,1	0	7346534	/tmp/vtePNT28W	(deleted)	
dconf	5833	5836	vdsq3226	56u	REG
252,1	0	7346535	/tmp/vte02I18W	(deleted)	
dbus	5833	5837	vdsq3226	21u	REG
252,1	20780	7342706	/tmp/vteLMXD9W	(deleted)	
dbus	5833	5837	vdsq3226	22u	REG
252,1	2504	7342710	/tmp/vteMGXD9W	(deleted)	
dbus	5833	5837	vdsq3226	23u	REG
252,1	0	7346448	/tmp/vteBBXD9W	(deleted)	
dbus	5833	5837	vdsq3226	24u	REG
252,1	458	7346484	/tmp/vteSLYW8W	(deleted)	
dbus	5833	5837	vdsq3226	25u	REG
252,1	24	7346485	/tmp/vte2MYW8W	(deleted)	
dbus	5833	5837	vdsq3226	26u	REG
252,1	8	7346486	/tmp/vteRPYW8W	(deleted)	
dbus	5833	5837	vdsq3226	29u	REG
252,1	34010	7346490	/tmp/vteR0ID9W	(deleted)	
dbus	5833	5837	vdsq3226	30u	REG
252,1	4096	7346494	/tmp/vte1TID9W	(deleted)	
dbus	5833	5837	vdsq3226	31u	REG
252,1	44074	7346495	/tmp/vteDM558W	(deleted)	

gdbus	5833	5837	vdsq3226	32u	REG
252,1	3656	7346496	/tmp/vte9U558W	(deleted)	
gdbus	5833	5837	vdsq3226	33u	REG
252,1	0	7346497	/tmp/vteTH3U8W	(deleted)	
gdbus	5833	5837	vdsq3226	34u	REG
252,1	0	7346498	/tmp/vteQF3U8W	(deleted)	
gdbus	5833	5837	vdsq3226	35u	REG
252,1	0	7346499	/tmp/vteRE3U8W	(deleted)	
gdbus	5833	5837	vdsq3226	36u	REG
252,1	128	7346500	/tmp/vteMMCX8W	(deleted)	
gdbus	5833	5837	vdsq3226	37u	REG
252,1	1526	7346501	/tmp/vte2NCX8W	(deleted)	
gdbus	5833	5837	vdsq3226	38u	REG
252,1	248	7346502	/tmp/vteK0CX8W	(deleted)	
gdbus	5833	5837	vdsq3226	41u	REG
252,1	2456	7346504	/tmp/vte9S6U8W	(deleted)	
gdbus	5833	5837	vdsq3226	42u	REG
252,1	312	7346505	/tmp/vteXU6U8W	(deleted)	
gdbus	5833	5837	vdsq3226	43u	REG
252,1	872	7346506	/tmp/vteXH6U8W	(deleted)	
gdbus	5833	5837	vdsq3226	44u	REG
252,1	64	7346522	/tmp/vteWZ658W	(deleted)	
gdbus	5833	5837	vdsq3226	45u	REG
252,1	218	7346523	/tmp/vteT1658W	(deleted)	
gdbus	5833	5837	vdsq3226	46u	REG
252,1	48	7346524	/tmp/vteG4658W	(deleted)	
gdbus	5833	5837	vdsq3226	49u	REG
252,1	24371	7346527	/tmp/vteJRJW8W	(deleted)	
gdbus	5833	5837	vdsq3226	50u	REG
252,1	2064	7346528	/tmp/vte5LJW8W	(deleted)	
gdbus	5833	5837	vdsq3226	51u	REG
252,1	12029	7346529	/tmp/vteVKS88W	(deleted)	
gdbus	5833	5837	vdsq3226	52u	REG
252,1	904	7346530	/tmp/vteDNS88W	(deleted)	
gdbus	5833	5837	vdsq3226	53u	REG
252,1	56568	7346532	/tmp/vte4WCB9W	(deleted)	
gdbus	5833	5837	vdsq3226	54u	REG
252,1	4096	7346533	/tmp/vteIVCB9W	(deleted)	
gdbus	5833	5837	vdsq3226	55u	REG
252,1	0	7346534	/tmp/vtePNT28W	(deleted)	
gdbus	5833	5837	vdsq3226	56u	REG
252,1	0	7346535	/tmp/vte02I18W	(deleted)	

gmain	5833	5839	vdsq3226	21u	REG
252,1	20780	7342706	/tmp/vteLMXD9W	(deleted)	
gmain	5833	5839	vdsq3226	22u	REG
252,1	2504	7342710	/tmp/vteMGXD9W	(deleted)	
gmain	5833	5839	vdsq3226	23u	REG
252,1	0	7346448	/tmp/vteBBXD9W	(deleted)	
gmain	5833	5839	vdsq3226	24u	REG
252,1	458	7346484	/tmp/vteSLYW8W	(deleted)	
gmain	5833	5839	vdsq3226	25u	REG
252,1	24	7346485	/tmp/vte2MYW8W	(deleted)	
gmain	5833	5839	vdsq3226	26u	REG
252,1	8	7346486	/tmp/vteR PYW8W	(deleted)	
gmain	5833	5839	vdsq3226	29u	REG
252,1	34010	7346490	/tmp/vteR0ID9W	(deleted)	
gmain	5833	5839	vdsq3226	30u	REG
252,1	4096	7346494	/tmp/vte1TID9W	(deleted)	
gmain	5833	5839	vdsq3226	31u	REG
252,1	44074	7346495	/tmp/vteDM558W	(deleted)	
gmain	5833	5839	vdsq3226	32u	REG
252,1	3656	7346496	/tmp/vte9U558W	(deleted)	
gmain	5833	5839	vdsq3226	33u	REG
252,1	0	7346497	/tmp/vteTH3U8W	(deleted)	
gmain	5833	5839	vdsq3226	34u	REG
252,1	0	7346498	/tmp/vteQF3U8W	(deleted)	
gmain	5833	5839	vdsq3226	35u	REG
252,1	0	7346499	/tmp/vteRE3U8W	(deleted)	
gmain	5833	5839	vdsq3226	36u	REG
252,1	128	7346500	/tmp/vteMMCX8W	(deleted)	
gmain	5833	5839	vdsq3226	37u	REG
252,1	1526	7346501	/tmp/vte2NCX8W	(deleted)	
gmain	5833	5839	vdsq3226	38u	REG
252,1	248	7346502	/tmp/vteK0CX8W	(deleted)	
gmain	5833	5839	vdsq3226	41u	REG
252,1	2456	7346504	/tmp/vte9S6U8W	(deleted)	
gmain	5833	5839	vdsq3226	42u	REG
252,1	312	7346505	/tmp/vteXU6U8W	(deleted)	
gmain	5833	5839	vdsq3226	43u	REG
252,1	872	7346506	/tmp/vteXH6U8W	(deleted)	
gmain	5833	5839	vdsq3226	44u	REG
252,1	64	7346522	/tmp/vteWZ658W	(deleted)	
gmain	5833	5839	vdsq3226	45u	REG
252,1	218	7346523	/tmp/vteT1658W	(deleted)	

gmain	5833	5839	vdsq3226	46u	REG
252,1	48	7346524	/tmp/vteG4658W	(deleted)	
gmain	5833	5839	vdsq3226	49u	REG
252,1	24371	7346527	/tmp/vteJRJW8W	(deleted)	
gmain	5833	5839	vdsq3226	50u	REG
252,1	2064	7346528	/tmp/vte5LJW8W	(deleted)	
gmain	5833	5839	vdsq3226	51u	REG
252,1	12029	7346529	/tmp/vteVKS88W	(deleted)	
gmain	5833	5839	vdsq3226	52u	REG
252,1	904	7346530	/tmp/vteDNS88W	(deleted)	
gmain	5833	5839	vdsq3226	53u	REG
252,1	56568	7346532	/tmp/vte4WCB9W	(deleted)	
gmain	5833	5839	vdsq3226	54u	REG
252,1	4096	7346533	/tmp/vteIVCB9W	(deleted)	
gmain	5833	5839	vdsq3226	55u	REG
252,1	0	7346534	/tmp/vtePNT28W	(deleted)	
gmain	5833	5839	vdsq3226	56u	REG
252,1	0	7346535	/tmp/vte02I18W	(deleted)	
mk_mirror	6191		vdsq3226	cwd	DIR
252,1	131072	9847067	/home/vdsq3226/bin/confdef/tmp		
cat	12551		vdsq3226	3r	FIFO
252,1	0t0	7346525	/tmp/f		
nc	12553		vdsq3226	1w	FIFO
252,1	0t0	7346525	/tmp/f		
grep	23032		vdsq3226	1w	REG
252,1	0	7346531	/tmp/log		

## Exemple avec lsof 2

version : 12-10-2014 18:03

lsof | grep "nc "

irqbalanc	1789		root	cwd	unknown
/proc/1789/cwd		(readlink: Permission denied)			
irqbalanc	1789		root	rtd	unknown
/proc/1789/root		(readlink: Permission denied)			
irqbalanc	1789		root	txt	unknown
/proc/1789/exe		(readlink: Permission denied)			
irqbalanc	1789		root	N0FD	
/proc/1789/fd		(opendir: Permission denied)			
nc	12553		vdsq3226	cwd	DIR

252,1	36864	9847066	/home/vdsq3226/bin/confdef		
nc	12553		vdsq3226	rtd	DIR
252,1	4096	2	/		
nc	12553		vdsq3226	txt	REG
252,1	30320	6815842	/bin/nc.openbsd		
nc	12553		vdsq3226	mem	REG
252,1	1779492	918831	/lib/i386-linux-gnu/libc-2.17.so		
nc	12553		vdsq3226	mem	REG
252,1	83816	918554	/lib/i386-linux-gnu/libresolv-2.17.so		
nc	12553		vdsq3226	mem	REG
252,1	55044	918345	/lib/i386-linux-gnu/libbsd.so.0.6.0		
nc	12553		vdsq3226	mem	REG
252,1	134376	918552	/lib/i386-linux-gnu/ld-2.17.so		
nc	12553		vdsq3226	0r	FIFO
0,8	0t0	68413	pipe		
nc	12553		vdsq3226	1w	FIFO
252,1	0t0	7346525	/tmp/f		
nc	12553		vdsq3226	2u	CHR
136,6	0t0	9	/dev/pts/6		
nc	12553		vdsq3226	4u	IPv4
68415	0t0	TCP	localhost:1234->localhost:53623		
(ESTABLISHED)					
nc	13223		vdsq3226	cwd	DIR
252,1	36864	9847066	/home/vdsq3226/bin/confdef		
nc	13223		vdsq3226	rtd	DIR
252,1	4096	2	/		
nc	13223		vdsq3226	txt	REG
252,1	30320	6815842	/bin/nc.openbsd		
nc	13223		vdsq3226	mem	REG
252,1	47080	918852	/lib/i386-linux-gnu/libnss_files-2.17.so		
nc	13223		vdsq3226	mem	REG
252,1	1779492	918831	/lib/i386-linux-gnu/libc-2.17.so		
nc	13223		vdsq3226	mem	REG
252,1	83816	918554	/lib/i386-linux-gnu/libresolv-2.17.so		
nc	13223		vdsq3226	mem	REG
252,1	55044	918345	/lib/i386-linux-gnu/libbsd.so.0.6.0		
nc	13223		vdsq3226	mem	REG

252,1	134376	918552	/lib/i386-linux-gnu/ld-2.17.so			
nc	13223		vdsq3226	0u	CHR	
136,9	0t0	12	/dev/pts/9			
nc	13223		vdsq3226	1u	CHR	
136,9	0t0	12	/dev/pts/9			
nc	13223		vdsq3226	2u	CHR	
136,9	0t0	12	/dev/pts/9			
nc	13223		vdsq3226	3u	IPv4	
70783	0t0	TCP	localhost:53623->localhost:1234			
(ESTABLISHED)						

Pour info: [Générer un serveur de shell](#)

## Analyse physique

version :

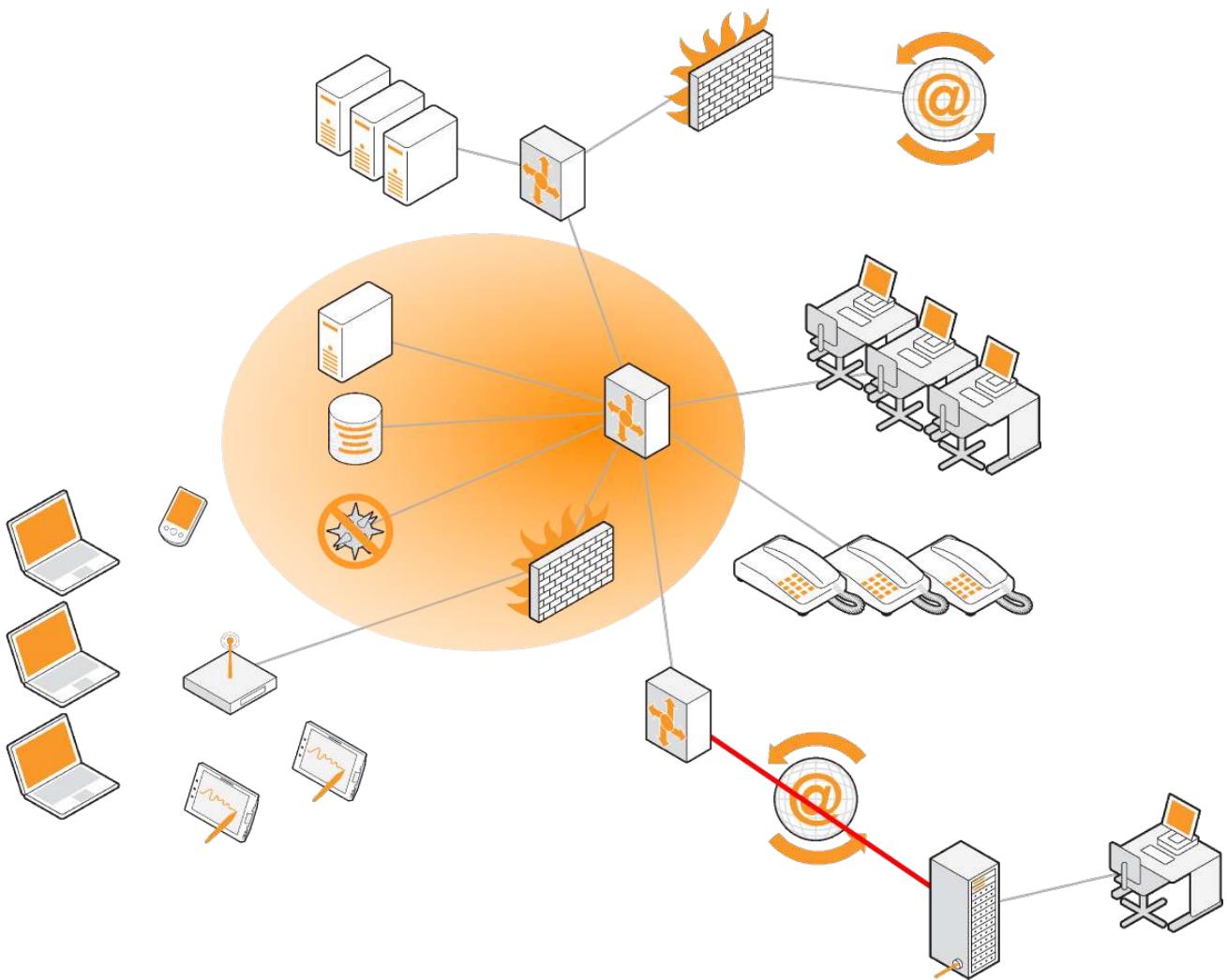
Missing tiddler "Analyse physique" - click  to create

## 4.4) Techniques Network

### Forensics

version : 06-10-2014 08:37

- C'est une analyse en "live"
- Pose de sniffer réseau
- Analyse de log (pare-feux, routeurs, ...)
- Analyse de mail
- Analyse d'historique de « chat », IRC, Web, ...



## 4.5) Techniques Social Forensics

version : 06-10-2014 08:39

Facebook, Twitter, Foursquare and Google Buzz

- de nombreux exploits sont signés sur Twitter
- @anonymousirc
- @lulsec
- ...

Il existe des cas où les réseaux sociaux ont été la source de l'enquête :

- [http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=3567](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3567)

M. L. a comparu à l'audience assisté de son conseil, il y a lieu de statuer contradictoirement à son égard.

Il est prévenu :

D'avoir à Bagnolet (93) et sur le territoire national, le 22 mars 2010 et depuis temps non prescrit, par un moyen de communication audiovisuelle, en l'espèce suite à la publication sur le site internet <http://www.viadeo.com> d'une fiche de membre créée au nom d'Eric R. contenant des imputations portant gravement atteinte à l'honneur et à la réputation de la société MMA Vie en raison des passages suivants : ...

Pour rire... (ou pas) :

PEBKAC #8903 par MrNumer0 J'explique à une amie qu'elle devrait faire plus attention aux données personnelles qu'elle laisse sur le Web. Je décide de lui faire une démonstration, en lui montrant des photos de ses soirées et des photos sexy d'elle-même, en faisant une simple recherche via Google Images :

« Je ne comprends pas, comment toutes ses données ont pu apparaître sur Internet ? Je ne l'utilise quasiment jamais ! – Mais tu utilises régulièrement les réseaux sociaux, non ? – Oui mais là c'est différent, je ne passe pas par Internet, vu que j'utilise des applications ! » PEBKAC.

## 4.6) Techniques Cloud Forensics

version : 09-12-2015 22:45

### Différences avec une analyse standard

- localisation du cloud :
  - d'un point de vue géographique
  - cloud public ou privé
- gestion du cloud
  - qui gère le cloud
  - externalisation de la gestion
- dépendances
  - dépendances avec d'autres infrastructures

# Dead Forensics

- copie bit-à-bit
  - facilité par le fait que les disques sont virtuels
  - facilité parce qu'ils sont accessibles (théoriquement) depuis n'importe où
  - facilité parce que la copie et la migration sont relativement faciles
  - difficulté vis-à-vis de la localisation physique des données
  - difficulté parce que le fournisseur de cloud ne fournit pas forcément d'interface pour récupérer les données des disques
- analyse
  - identique à une analyse standard

# Live Forensics

- copie bit-à-bit
  - facilité par l'utilisation de la mise en pause
  - difficulté parce que le fournisseur de cloud ne fournit pas forcément d'interface pour récupérer les données
- analyse
  - identique à une analyse standard

# Network Forensics

- la pause de sniffer réseau est facilitée par les NFV
- la coupure ou la modification du routage est beaucoup plus simple que pour un réseau "standard"
- l'analyse des logs est identique à une analyse standard

## 5) Outils

version : 16-12-2015 09:34

[TableOfContents](#)

Sommaire:

- Live-CD
- Framework

- Station portable
- Outils :
  - Outils Dead Forensics
  - Outils Live Forensics
  - Outils Network Forensics
  - Outils Social Forensics

## 5.1) Live-CD

version : 17-02-2017 18:25

Helix

SANS SIRT Workstation

CAINE

DEFT

## Helix

version : 17-02-2017 18:24

### Version 3

<http://www.e-fense.com/products.php>

Live CD et Live USB



- Sleuthkit
- EnCase LinEn Utility
- Libewf + mount\_ewf
- Carvfs
- cryptsetup
- Truecrypt
- lvm2
- Scalpel
- Foremost
- LibPff
- Volatility plus many plugins
- moto4lin
- gmobilemedia
- gammu
- gnokii
- frag\_find
- pythonraw
- ptfinder

# SANS SIRT Workstation

version : 17-02-2017 11:17

<http://computer-forensics.sans.org/community/downloads>

La version actuelle est la 3

Voici la liste des caractéristiques principales.

## File system support

- ntfs (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- raw (Raw Data)
- swap (Swap Space)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)
- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)
- vmdk

## Evidence Image Support

- raw (Single raw file (dd))
- aff (Advanced Forensic Format)
- afd (AFF Multiple File)
- afm (AFF with external metadata)
- afflib (All AFFLIB image formats (including beta ones))
- ewf (Expert Witness format (encase))
- split raw (Split raw files) via affuse
- affuse \0x2010 mount 001 image/split images to view single raw file and metadata
- split ewf (Split E01 files) via mount\_ewf.py

- mount\_ewf.py \0x2010 mount E01 image/split images to view single raw file and metadata
- ewfmount - mount E01 images/split images to view single rawfile and metadata

## Incident Response Support

- F-Response Tool Suite Compatible
- Rapid Scripting and Analysis
- Threat Intelligence and Indicator of Compromise Support
- Threat Hunting and Malware Analysis Capabilities

## Partition Table Support

- dos (DOS Partition Table)
- mac (MAC Partition Map)
- bsd (BSD Disk Label)
- sun (Sun Volume Table of Contents (Solaris))
- gpt (GUID Partition Table (EFI))

## Software Includes:

- log2timeline (Timeline Generation Tool)
- Rekall Framework (Memory Analysis)
- Volatility Framework (Memory Analysis)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)
  - afflib
    - afflib-tools
- libbde
- libesedb
- libevt
- libevtx
- libewf
  - libewf-tools
  - libewf-python
- libfvde
- libvshadow
- log2timeline

- Plaso
- qemu
- **SleuthKit**
- 100s more tools



# CAINE

version : 17-02-2017 18:25

## Version 8.0

<http://www.caine-live.net/>

Basé sur le Kernel 4.4.0-45 et Ubuntu 16.04 64 bits

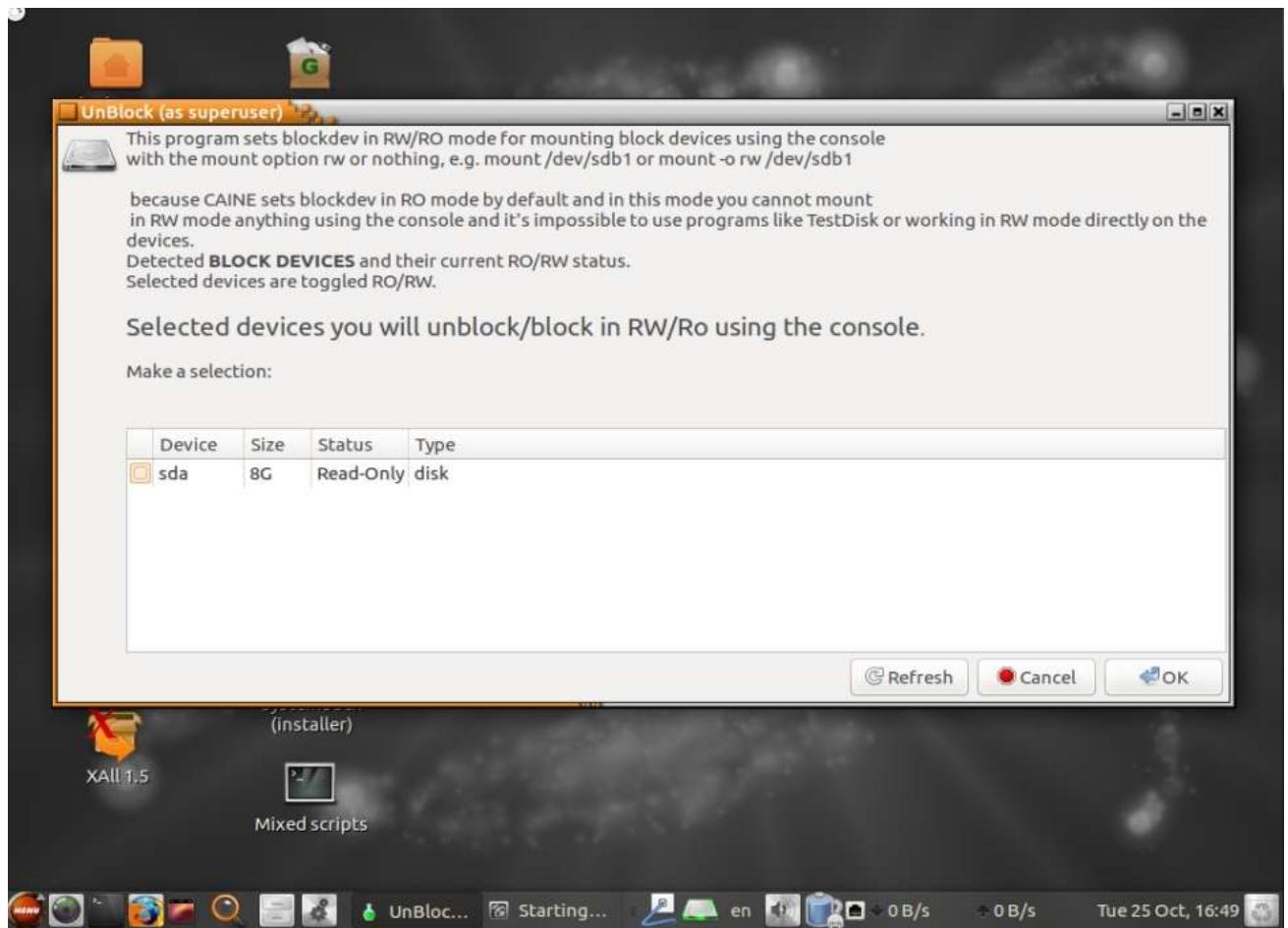
Report creation procedure

Autopsy	Interface graphique de Sleuth Kit
Afflib	Format ouvert pour la conservation des preuves
Ataraw	Utilitaires pour envoyer des commandes bas niveau ATA
Bkhive	Extracteur de Hash Windows
Bulk Extractor	Extracteur de mails
Ddrescue	Outil pour la copie de disques
Dcfldd	Outil pour la copie de disques

dc3dd	Outil pour la copie de disques
Foremost	Récupération de données selon leur entête
FiWalk	Outil pour l'analyse des fichiers et des inodes
Fatback	Récupérateur de données pour système de fichier FAT
Win UFO	Utilitaires sous Windows







# DEFT

version : 17-02-2017 18:25

**Version 2017.1**



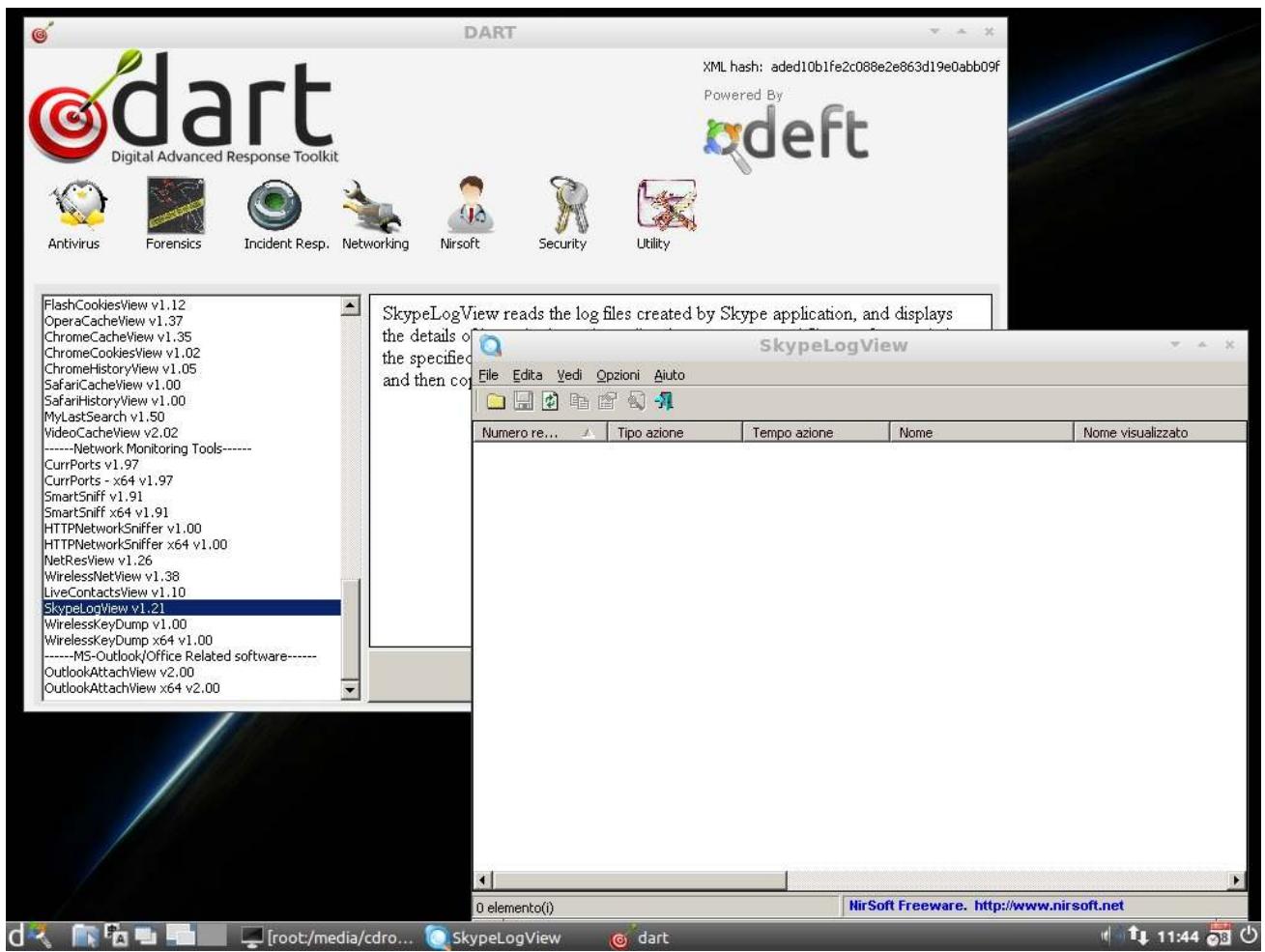
<http://www.deftlinux.net/>

Basé sur [Ubuntu](#)

Linux kernel 3.0.0-12, USB 3 ready	Dropbox Reader
Libewf 20100226	Emule Forensic 1.0
Afflib 3.6.14	Guymager 0.6.3-1
TSK 3.2.3	Dhash 2
Autopsy 2.24	Cyclone wizard acquire tool
Digital Forensic Framework 1.2	lpddump
PTK Forensic 1.0.5 DEFT edition	Iphone Analyzer
Pyflag	Iphone backup analyzer
Maltego CE	~SQLite Database Browser 2.0b1
KeepNote 0.7.6	BitPim 1.0.7
Mobius Forensic	Bbwhatsapp database converter
Xplico 0.7.1	Regripper
Scalpel 2	Creepy 0.1.9
Hunchbackeed Foremost 0.6	Hydra 7.1
Findwild 1.3	Log2timeline 0.60
Bulk Extractor 1.1	Wine 1.3.28



DEFT possède aussi un ensemble d'utilitaires Windows :



## 5.3) Station portable

version : 08-01-2015 23:00

# Forensics Mobile Workstation

<http://www.forensic-computers.com/fmw2.php>



## TRACIP

<http://www.tracip.fr>





**SOLO 101**

La solution mobile de duplication forensique. Duplication 1 : 1. Compatible IDE, SATA et USB. Stockage réseau Gigabit

>[En savoir plus](#)



**UFED Touch Ultimate**

Solutions d'investigation Numérique de téléphone mobiles entièrement intégrées

>[En savoir plus](#)

## 5.4) Outils Dead Forensics

version : 06-10-2014 08:52

Disques en clair

Disques chiffrés

## Disques en clair

version : 17-02-2017 17:56

## Multi-système

Sleuthkit

Foremost

Encase

Timeline Analysis

## Linux

Lire les fichiers PST Outlook

## Collection de scripts pour Linux

# Windows

## Analyse de la base de registre

[RegRipper](#) is an open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis.

Analyse automatique de fichiers exe, doc, ...

# Sleuthkit

version : 17-02-2017 11:40

<http://www.sleuthkit.org/>

Sleuthkit fonctionne sous :

- Linux
- Mac OS X
- Windows
- CYGWIN
- Open & FreeBSD
- Solaris

Il est capable de lire les systèmes de fichiers suivants :

- NTFS
- EXT2FS,
- EXT3FS,
- FAT
- UFS 1
- UFS 2
- ISO 9660

Liste des outils contenu dans Sleuthkit :

img_cat	ifind	blkcalc	srch_strings
img_stat	istat	blkcat	sigfind

mmls	jcat	blkls	sorter
mmstat	jls	blkstat	icat-sleuthkit
mmcatt	hfind	ffind	ils-sleuthkit
fsstat	fls	mactime-sleuthkit	

# Autopsy

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Allocated
\$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Allocated
\$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Allocated
\$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Allocated
\$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Allocated
\$Secure:\$SSD	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
\$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Allocated
\$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:20:54	2012-01-20 17:20:10	211	Allocated	Allocated
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Allocated
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Allocated
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Allocated
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Allocated
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Allocated
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated

# Foremost

version : 06-10-2014 08:55

<http://foremost.sourceforge.net>

Logiciel permettant de faire du "data carving"

Pour retrouver des données, il se base sur :

- les entêtes
- les fins de fichiers
- leur structure interne

```
audit.txt doc gif jpg mov pdf ppt wav wmv xls zip
```

## Encase

version : 06-10-2014 08:56

<http://www.guidancesoftware.com/>

- Gestion des enquêtes
- Acquisition de preuve
- Traitement des preuves
- Recherche et Analyse
- Identifications des éléments pertinents
- Génération de rapports

**EnCase Enterprise Training**

- Case (Harrison Investigation)
- View
- Tools
- Enterprise
- EnScript
- Add Evidence

**Home**

Zoom In Zoom Out 100%

**RECENT CASES**

- Harrison Investigation
- Whiteford Investigation
- 7.06 Demo
- Tech Forum

**CASE FILE**

- New Case Create a new case
- Open Open an existing case

**ENTERPRISE**

- Logon Logon to SAFE

**VIEW**

- EnScripts Installed EnScripts
- Generate Encryption Key Generates an Encryption Key
- Options Change global options and settings
- File Types Display File Types table

**EnCase Enterprise Training**

- Case (Tech Forum 707147)
- View
- Tools
- Enterprise
- EnScript
- Add Evidence

**Records**

**Viewing (Record) - Selected 0/1058**

Name	Tag	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag
1 outlook.ost		ost	0	Document	Folder			
2 tdurden1263@gmail.com.pst		pst	0	Document	Folder			
3 tdurden1263@gmail.com.pst		pst	0	Document	Folder			
4 Outlook.pst		pst	0	Document	Folder			
5 DeniseGreen.pst		pst	0	Document	Folder			
6 Outlook.pst		pst	0	Document	Folder			
7 BrendaSmith.pst		pst	0	Document	Folder			
8 CharlesDoe.pst		pst	0	Document	Folder			
9 FranklinBrown.pst		pst	0	Document	Folder			

**Report Text Hex Decode Doc Transcript Picture Console Fields**

Zoom In Zoom Out 100% Previous Item Next Item

Name	outlook.ost
File Ext	ost
Logical Size	0
Item Type	Document
Category	Folder
Primary Device	TDurden
Item Path	outlook.ost

# Timeline Analysis

version : 17-02-2017 18:01

Plaso est un moteur pour l'outil *log2timeline*.

*log2timeline* est un outil permettant d'extraire les *timestamps* de nombreux fichiers puis de les agréger.

<http://plaso.kiddaland.net/>

# Lire les fichiers PST Outlook

version : 08-01-2015 23:02

<http://dereknewton.com/2011/02/searching-and-extracting-data-from-pst-files/>

L'outil *readpst* permet d'extraire les communications d'un fichier PST :

```
sudo apt-get install readpst  
readpst -S -o out/ outlook.pst
```

Cet outil permet d'exporter un fichier binaire PST :

```
$ file archive.pst  
archive.pst: Microsoft Outlook email folder (>=2003)
```

en plusieurs fichiers au format mbox facilement utilisable sous Linux.

```
$ file Archives.sbd/mbox  
Archives.sbd/mbox: Non-ISO extended-ASCII text, with  
very long lines
```

# Collection de scripts pour Linux

version : 08-01-2015 23:02

<http://scripts4cf.sourceforge.net/tools.html>

# Analyse automatique de fichiers exe, doc, ...

version : 09-12-2015 18:58

Certaines applications permettent de faire de l'analyse automatique de malware.

## Cuckoo

via <http://anupriti.blogspot.in/2015/09/cuckoo-sandboxautomatic-malware.html>

Cuckoo permet d'analyser dans un "bac à sable" des executables douteux en quelques secondes.

### **Cuckoo can produce the following types of results:**

- Files being created, deleted, and downloaded by the malware during its execution
- Network traffic trace in PCAP format(as we get with wireshark and ethereal)
- Traces of win32 API calls spawned by the malware
- Memory dumps of the malware processes
- Screenshots of the Windows desktop as it happens during execution of the malware
- Full memory dumps of the machines

### **The following kinds of files can be analysed and put for check in cuckoo :**

- DLL files
- Windows executables ie .exe
- Microsoft Office docs

- URLs
- Typical PDF documents
- PHP scripts
- Anything actually!!!

cuckoo@maanikbaasha: /opt/cuckoo  
Interrupt:19  
cuckoo@maanikbaasha:/opt/cuckoo\$ ./cuckoo.py

Cuckoo Sandbox 2.0-dev  
www.cuckosandbox.org  
Copyright (c) 2010-2015

Checking for updates...  
Good! You have the latest version available.

```
2015-09-15 20:46:41,271 [root] WARNING: The binary analyzer/windows/bin/monitor-x86.dll is more than a week old!  
2015-09-15 20:46:41,333 [root] WARNING: The binary analyzer/Windows/bin/monitor-x64.dll is more than a week old!  
2015-09-15 20:46:41,353 [root] WARNING: The binary analyzer/windows/bin/inject-x86.exe is more than a week old!  
2015-09-15 20:46:41,367 [root] WARNING: The binary analyzer/windows/bin/inject-x64.exe is more than a week old!  
2015-09-15 20:46:41,379 [root] WARNING: The binary analyzer/windows/bin/is32bit.exe is more than a week old!  
2015-09-15 20:46:41,380 [root] CRITICAL: It is recommended that you update the binaries used for Windows analysis (if you have not done so already, it is possible that there was no update - in that case this error will persist). To do so, please run the following command: ./utils/commonty.py -wafb monitor  
2015-09-15 20:46:41,383 [lib.cuckoo.core.scheduler] INFO: Using "virtualbox" machine manager with max_analysis_count=0, max_machines_count=0, and max_vmstartup_count=10  
2015-09-15 20:46:43,859 [lib.cuckoo.core.scheduler] INFO: Loaded 1 machine/s  
2015-09-15 20:46:43,870 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis tasks.  
2015-09-15 20:46:45,070 [lib.cuckoo.core.scheduler] INFO: Starting analysis of FILE "/home/cuckoo/Desktop/cuccccc/shared/Cuckoo Malware Analysis.pdf" (task=1)  
2015-09-15 20:46:45,575 [lib.cuckoo.core.scheduler] INFO: Task #1: acquired machine cuckoo1 (label=cuckoo1)  
2015-09-15 20:46:45,615 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 8096 (interface=vboxnet0, host=192.168.56.101, dump path=/opt/cuckoo/storage/analyses/1/dump.pcap)
```

cuckoo@maanikbaasha: ~  
cuckoo@maanikbaasha:~\$ python /opt/cuckoo/utils/submit.py /home/cuckoo/Desktop/cuccccc/shared/malware.pdf  
**Success:** File "/home/cuckoo/Desktop/cuccccc/shared/malware.pdf" added as task with ID 6  
cuckoo@maanikbaasha:~\$

The screenshot shows the Cuckoo Sandbox web interface. At the top, there are several tabs: 'Blogger: MELIORATI', 'Install CuckooBox fo...', 'Inbox - anupam605', 'Cuckoo Sandbox', and others. Below the tabs, the address bar shows '0.0.0.0:8080'. A message says 'For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...'. There are 'Home' and 'Browse' buttons. The main content area features a large 'cuckoo' logo with a bird. Below it, the text 'New Analysis' is displayed, followed by the sub-instruction 'use this form to add a new analysis task'. The form contains the following fields:

- File to upload: A button labeled 'Choose File' with the text 'No file chosen'.
- Package to use: An empty input field.
- Options: An empty input field.
- Timeout: An empty input field.
- Priority: A dropdown menu set to 'Low'.
- Machine: A dropdown menu set to 'Any'.
- Capture Memory: A dropdown menu set to 'False'.

At the bottom of the form are two buttons: 'Submit' (highlighted in blue) and 'Cancel'.

## Disques chiffrés

version : 06-10-2014 08:57

Il faut être capable de déchiffrer les disques, il y a plusieurs moyens :

- utiliser une vulnérabilité de l'utilitaire de chiffrement
- récupérer la clé de chiffrement
  - via la RAM comme pour [Elcomsoft Forensic Disk Decryptor](#)

## 5.5) Outils Live Forensics

version : 09-12-2015 22:48

## Volatility

Permet d'analyser la mémoire des systèmes Windows et Linux et Mac (en étant sous Linux).

- Volatility - Windows
- Volatility - Linux
- Volatility - Mac
- Volatility - Malwares
- Volatility - VMWare

[http://downloads.volatilityfoundation.org/releases/2.4/CheatSheet\\_v2.4.pdf](http://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf)

[https://alexandreborgesbrazil.files.wordpress.com/2015/02/memory\\_acquisition\\_1-2.pdf](https://alexandreborgesbrazil.files.wordpress.com/2015/02/memory_acquisition_1-2.pdf)

## draugr

<http://code.google.com/p/draugr/> Projet mort ? En utilisant /dev/(k)mem ou un dump mémoire, Draugr peut être utilisé pour accéder facilement via python à cette mémoire pour

- lire, écrire, démonter, recherche
- trouver des informations système (processus ...)

## Inception

<http://www.breaknenter.org/projects/inception/>

permet la récupération de la mémoire RAM des systèmes Windows par une simple connexion sur un port Firewire.

La même chose pour linux : <https://freddie.witherden.org/tools/libforensic1394/>

## PyPMF

<https://github.com/feliam/PyPMF> "A small python module to manipulate Windows Internals Process Monitor PMF Filter files"

# MoonSols Windows Memory Toolkit

<http://www.moonsols.com/products/> MoonSols permet l'acquisition de mémoire de systèmes Windows

- ~VMWare memory snapshot,
- Microsoft crash dump et
- Windows hibernation file

MoonSols permet la conversion vers Microsoft Windows Debugg \*

<http://www.microsoft.com/whdc/Devtools/Debugging/default.mspx>

# Forensic Analysis Toolkit FaTkit

<http://www.4tphi.net/fatkit/>

- Support des processeurs X86
- Support des noyau Linux et Windows

# Microsoft Cofee

<http://www.microsoft.com/industry/government/solutions/cofee/default.aspx>

Cofee permet de construire sur une clé USB une compilation d'outils de collecte de données lors d'une intervention par un enquêteur sur un ordinateur allumé. Il est diffusé exclusivement auprès des services policiers dans le monde entier, notamment au travers d'Interpol.

# GRR

<https://code.google.com/p/grr>



GRR Rapid Response is an incident response framework focused on remote

live forensics.

# Volatility - Windows

version : 08-01-2015 23:03

<http://code.google.com/p/volatility/wiki/CommandReference23>

Liste des commandes possibles :

- **Image Identification** ( imageinfo kdbgscan kpcrscan )
- **Processes and ~DLLs** ( pslist pstree psscan psdispscan dlllist dlldump handles getsids cmdscan consoles privs envars verinfo enumfunc )
- **Process Memory** ( memmap memdump procmemdump procededump vadinfo vadwalk vadtree vaddump evtlogs iehistory )
- **Kernel Memory and Objects** ( modules modscan moddump ssdt driverscan filescan mutantscan symlinkscan thrdscan dumpfiles unloadedmodules )
- **Networking** ( connections connscan sockets sockscan netscan )
- **Registry** ( hivescan hivelist printkey hivedump hashdump lsadump userassist shellbags shimcache getservicesids )
- **Crash Dumps, Hibernation, and Conversion** ( crashinfo hibinfo imagecopy raw2dmp vboxinfo vmwareinfo hpakinfo hpakextract )
- **File System** ( mbrparser mftparse r )
- **Miscellaneous** ( strings volshell bioskbd patcher pagecheck timeliner )

Exemple :

```
$ python vol.py -f ~/Desktop/win7_trial_64bit.raw
--profile=Win7SP0x64 pslist
Volatile Systems Volatility Framework 2.1 alpha
Offset(V)           Name                  PID  PPID
Thds      Hnds   Sess  Wow64 Start          Exit
-----
-----
-----
0xfffffa80004b09e0 System                 4    0
78        489  -----  0 2012-02-22 19:58:20
0xfffffa8000ce97f0 smss.exe               208   4
2         29   -----  0 2012-02-22 19:58:20
0xfffffa8000c006c0 csrss.exe              296   288
9         385     0   0 2012-02-22 19:58:24
```

0xfffffa8000c92300	wininit.exe	332	288
3	74	0	0 2012-02-22 19:58:30
0xfffffa8000c06b30	csrss.exe	344	324
7	252	1	0 2012-02-22 19:58:30
0xfffffa8000c80b30	winlogon.exe	372	324
5	136	1	0 2012-02-22 19:58:31
0xfffffa8000c5eb30	services.exe	428	332
6	193	0	0 2012-02-22 19:58:32
0xfffffa80011c5700	lsass.exe	444	332
6	557	0	0 2012-02-22 19:58:32
0xfffffa8000ea31b0	lsm.exe	452	332
10	133	0	0 2012-02-22 19:58:32
0xfffffa8001296b30	svchost.exe	568	428
10	352	0	0 2012-02-22 19:58:34
0xfffffa80012c3620	svchost.exe	628	428
6	247	0	0 2012-02-22 19:58:34
0xfffffa8001325950	sppsvc.exe	816	428
5	154	0	0 2012-02-22 19:58:41
0xfffffa80007b7960	svchost.exe	856	428
16	404	0	0 2012-02-22 19:58:43
0xfffffa80007bb750	svchost.exe	880	428
34	1118	0	0 2012-02-22 19:58:43
0xfffffa80007d09e0	svchost.exe	916	428
19	443	0	0 2012-02-22 19:58:43
0xfffffa8000c64840	svchost.exe	348	428
14	338	0	0 2012-02-22 20:02:07
0xfffffa8000c09630	svchost.exe	504	428
16	496	0	0 2012-02-22 20:02:07
0xfffffa8000e86690	spoolsv.exe	1076	428
12	271	0	0 2012-02-22 20:02:10
0xfffffa8000518b30	svchost.exe	1104	428
18	307	0	0 2012-02-22 20:02:10
0xfffffa800094d960	wlms.exe	1264	428
4	43	0	0 2012-02-22 20:02:11
0xfffffa8000995b30	svchost.exe	1736	428
12	200	0	0 2012-02-22 20:02:25
0xfffffa8000aa0b30	SearchIndexer.	1800	428
12	757	0	0 2012-02-22 20:02:26
0xfffffa8000aea630	taskhost.exe	1144	428
7	189	1	0 2012-02-22 20:02:41
0xfffffa8000eafb30	dwm.exe	1476	856
3	71	1	0 2012-02-22 20:02:41

0xfffffa80008f3420	explorer.exe	1652	840
21	760	1	0 2012-02-22 20:02:42
0xfffffa8000c9a630	regsvr32.exe	1180	1652
0	-----	1	0 2012-02-22 20:03:05
<b>2012-02-22 20:03:08</b>			
0xfffffa8000a03b30	rundll32.exe	2016	568
3	67	1	0 2012-02-22 20:03:16
0xfffffa8000a4f630	svchost.exe	1432	428
12	350	0	0 2012-02-22 20:04:14
0xfffffa8000999780	iexplore.exe	1892	1652
19	688	1	1 2012-02-22 11:26:12
0xfffffa80010c9060	iexplore.exe	2820	1892
23	733	1	1 2012-02-22 11:26:15
0xfffffa8001016060	DumpIt.exe	2860	1652
2	42	1	1 2012-02-22 11:28:59
0xfffffa8000acab30	conhost.exe	2236	344
2	51	1	0 2012-02-22 11:28:59

## Volatility - Linux

version : 08-01-2015 23:05

## Linux

<http://code.google.com/p/volatility/wiki/LinuxMemoryForensics>

<http://www.unixgarden.com/index.php/misc/challenge-sstic-et-analyse-de-la-memoire-physique-des-systemes-linux>

Le plus important sous Linux c'est qu'il faut créer un profil qui correspond au profil que l'on va analyser. Un profil contient notamment les structures de données du noyau ainsi que les symboles de débogage.

Exemple :

```
sudo zip volatility/volatility/plugins/overlays/linux
/Ubuntu1204.zip volatility/tools/linux/module.dwarf
/boot/System.map-3.2.0-23-generic
adding: volatility/tools/linux/module.dwarf
(deflated 89%)
```

adding: boot/System.map-3.2.0-23-generic (deflated  
79%)

Les commandes disponibles sont les suivantes :

- linux\_arp - Print the ARP table
- linux\_bash - Recover bash history from bash process memory
- linux\_check\_afinfo - Verifies the operation function pointers of network protocols
- linux\_check\_creds - Checks if any processes are sharing credential structures
- linux\_check\_fop - Check file operation structures for rootkit modifications
- linux\_check\_idt - Checks if the IDT has been altered
- linux\_check\_modules - Compares module list to sysfs info, if available
- linux\_check\_syscall - Checks if the system call table has been altered
- linux\_cpuinfo - Prints info about each active processor
- linux\_dentry\_cache - Gather files from the dentry cache
- linux\_dmesg - Gather dmesg buffer
- linux\_dump\_map - Writes selected memory mappings to disk
- linux\_find\_file - Recovers tmpfs filesystems from memory
- linux\_ifconfig - Gathers active interfaces
- linux\_iomem - Provides output similar to /proc/iomem
- linux\_lsmod - Gather loaded kernel modules
- linux\_lsof - Lists open files
- linux\_memmap - Dumps the memory map for linux tasks
- linux\_mount - Gather mounted fs/devices
- linux\_mount\_cache - Gather mounted fs/devices from kmem\_cache
- linux\_netstat - Lists open sockets
- linux\_pidhashtable - Enumerates processes through the PID hash table
- linux\_pkt\_queues - Writes per-process packet queues out to disk
- linux\_proc\_maps - Gathers process maps for linux
- linux\_psaux - Gathers processes along with full command line and start time
- linux\_pslist - Gather active tasks by walking the task\_struct->task list
- linux\_pslist\_cache - Gather tasks from the kmem\_cache
- linux\_pstree - Shows the parent/child relationship between processes
- linux\_psxview - Find hidden processes with various process listings
- linux\_route\_cache - Recovers the routing cache from memory
- linux\_sk\_buff\_cache - Recovers packets from the sk\_buff kmem\_cache
- linux\_slabinfo - Mimics /proc/slabinfo on a running machine
- linux\_tmpfs - Recovers tmpfs filesystems from memory

- linux\_vma\_cache - Gather ~VMAs from the vm\_area\_struct cache

## Volatility - Mac

version : 08-01-2015 23:05

<http://code.google.com/p/volatility/wiki/MacCommandReference23>

- **Processes** ( mac\_pslist mac\_tasks mac\_pstree mac\_lsof mac\_pgrp\_hash\_table mac\_pid\_hash\_table mac\_psaux mac\_dead\_procs mac\_psxview )
- **Process Memory** ( mac\_proc\_maps mac\_dump\_maps )
- **Kernel Memory and Objects** ( mac\_list\_sessions mac\_list\_zones mac\_lsmod mac\_mount )
- **Networking** ( mac\_arp mac\_ifconfig mac\_netstat mac\_route )
- **Malware/Rootkits** ( mac\_check\_sysctl mac\_check\_syscalls mac\_check\_trap\_table mac\_ip\_filters mac\_notifiers mac\_trustedbsd )
- **System Information** ( mac\_dmesg mac\_find\_aslr\_shift mac\_machine\_info mac\_version mac\_print\_boot\_cmdline )
- **Miscellaneous** ( mac\_volshell mac\_yarascan )

## Volatility - Malwares

version : 08-01-2015 23:05

<http://code.google.com/p/volatility/wiki/CommandReferenceMal23>

Volatility permet de détecter des malwares, virus, cheval de Troie, ...

- malfind
- yarascan
- svcscan
- ldrmodules
- impscan
- apihooks
- idt
- gdt
- threads
- callbacks
- driverirp
- devicetree
- psxview

- timers

Exemple :

```
$ python vol.py -f silentbanker.vmem -p 1884 apihooks
Volatile Systems Volatility Framework 2.1 alpha
*****
*****
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1884 (IEXPLORE.EXE)
Victim module: kernel32.dll (0x7c800000 - 0x7c8f4000)
Function: kernel32.dll!ExitProcess at 0x7c81caa2
Hook address: 0xe50000
Hooking module: <unknown>

Disassembly(0):
0x7c81caa2 e959356384      JMP 0xe50000
0x7c81caa7 6aff             PUSH -0x1
0x7c81caa9 68b0f3e877      PUSH DWORD 0x77e8f3b0
0x7c81caae ff7508          PUSH DWORD [EBP+0x8]
0x7c81cab1 e846ffffff     CALL 0x7c81c9fc

Disassembly(1):
0xe50000 58                 POP EAX
0xe50001 680500e600          PUSH DWORD 0xe60005
0xe50006 6800000000          PUSH DWORD 0x0
0xe5000b 680000807c          PUSH DWORD 0x7c800000
0xe50010 6828180310          PUSH DWORD 0x10031828
0xe50015 50                 PUSH EAX

[snip]
```

## Volatility - VMWare

version : 08-01-2015 23:06

<http://code.google.com/p/volatility/wiki/VMwareSnapshotFile>

Volatility peut analyser les VMs sauvegardées (.vmss) les snapshots (.vmsn).

Exemple :

```
$ python vol.py -f ~/Desktop/Win7SP1x64-d8737a34.vmss  
vmwareinfo --verbose | less
```

Magic: 0xbad1bad1 (Version 1)  
Group count: 0x5c

File Offset PhysMem Offset Size

File	Offset	PhysMem	Offset	Size
	0x000010000	0x00000000000000	0xc0000000	
	0x0c0010000	0x000100000000	0xc0000000	

DataOffset DataSize Name

Value

DataOffset	DataSize	Name
0x00001cd9	0x4	Checkpoint/fileversion
0xa		
0x00001cfcc	0x100	Checkpoint/ProductName
0x00001cfcc	56 4d 77 61 72 65 20 45 53 58 00 00 00 00 00 00	VMware.ESX.....
0x00001d0c	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00		
[snip]		
0x00001e1d	0x100	Checkpoint/VersionNumber
0x00001e1d	34 2e 31 2e 30 00 00 00 00 00 00 00 00 00 00 00	4.1.0.....
0x00001e2d	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00		
[snip]		
0x00002046	0x4	Checkpoint/Platform
0x1		
0x00002055	0x4	Checkpoint/usageMode
0x1		
0x00002062	0x4	Checkpoint/memSize
0x1800		
0x00002071	0x4	Checkpoint/maxFBSIZE
0x800000		
0x00002085	0x4	cpu/cpu:numVCPU
0x1		
0x00002095	0x4	cpu/eFLAGS[0]
0x86		

0x000020a2	0x8 cpu/rip[0]
0xfffff80002c1c0ba	
0x000020b3	0x4 cpu/eip[0]
0x2c1c0ba	
0x000020c3	0x1 cpu/halted[0]
0	
[snip]	
0x00005eea	0x4 cpu/CR[0][0]
0x80050031	
0x00005efa	0x4 cpu/CR[0][1]
0x0	
0x00005f0a	0x4 cpu/CR[0][2]
0x865eb08	
0x00005f1a	0x4 cpu/CR[0][3]
0x187000	
0x00005f2a	0x4 cpu/CR[0][4]
0x6f8	
0x00005f3c	0x8 cpu/DR64[0][0]
0x0	
[snip]	
0x00006020	0x8 cpu/DR64[0][6]
0xfffff0ff0	
0x00006034	0x4 cpu/DR[0][6]
0xfffff0ff0	
0x00006046	0x8 cpu/DR64[0][7]
0x400	
0x0000605a	0x4 cpu/DR[0][7]
0x400	
0x0000606c	0x2 cpu/GDTR[0][0]
127	
0x0000607c	0x4 cpu/GDTR[0][1]
0x3cd5000	
0x0000608e	0x4 cpu/GDTR[0][2]
0xfffff800	
0x000060a0	0x2 cpu/IDTR[0][0]
4095	
0x000060b0	0x4 cpu/IDTR[0][1]
0x3cd5080	
0x000060c2	0x4 cpu/IDTR[0][2]
0xfffff800	
[snip]	
0x180011963	0x2c29 Snapshot/cfgFile

```
0x180011953 2e 65 6e 63 6f 64 69 6e 67 20 3d 20 22 55  
54 46 .encoding.=."UTF  
0x180011963 2d 38 22 0a 63 6f 6e 66 69 67 2e 76 65 72  
73 69 -8".config.versi  
0x180011973 6f 6e 20 3d 20 22 38 22 0a 76 69 72 74 75  
61 6c on.=."8".virtual  
0x180011983 48 57 2e 76 65 72 73 69 6f 6e 20 3d 20 22  
37 22 HW.version.=."7"  
0x180011993 0a 70 63 69 42 72 69 64 67 65 30 2e 70 72  
65 73 .pciBridge0.pres  
0x1800119a3 65 6e 74 20 3d 20 22 74 72 75 65 22 0a 70  
63 69 ent.=."true".pci  
0x1800119b3 42 72 69 64 67 65 34 2e 70 72 65 73 65 6e  
74 20 Bridge4.present.  
0x1800119c3 3d 20 22 74 72 75 65 22 0a 70 63 69 42 72  
69 64 =."true".pciBrid  
0x1800119d3 67 65 34 2e 76 69 72 74 75 61 6c 44 65 76  
20 3d ge4.virtualDev.=  
0x1800119e3 20 22 70 63 69 65 52 6f 6f 74 50 6f 72 74  
22 0a ."pcieRootPort".
```

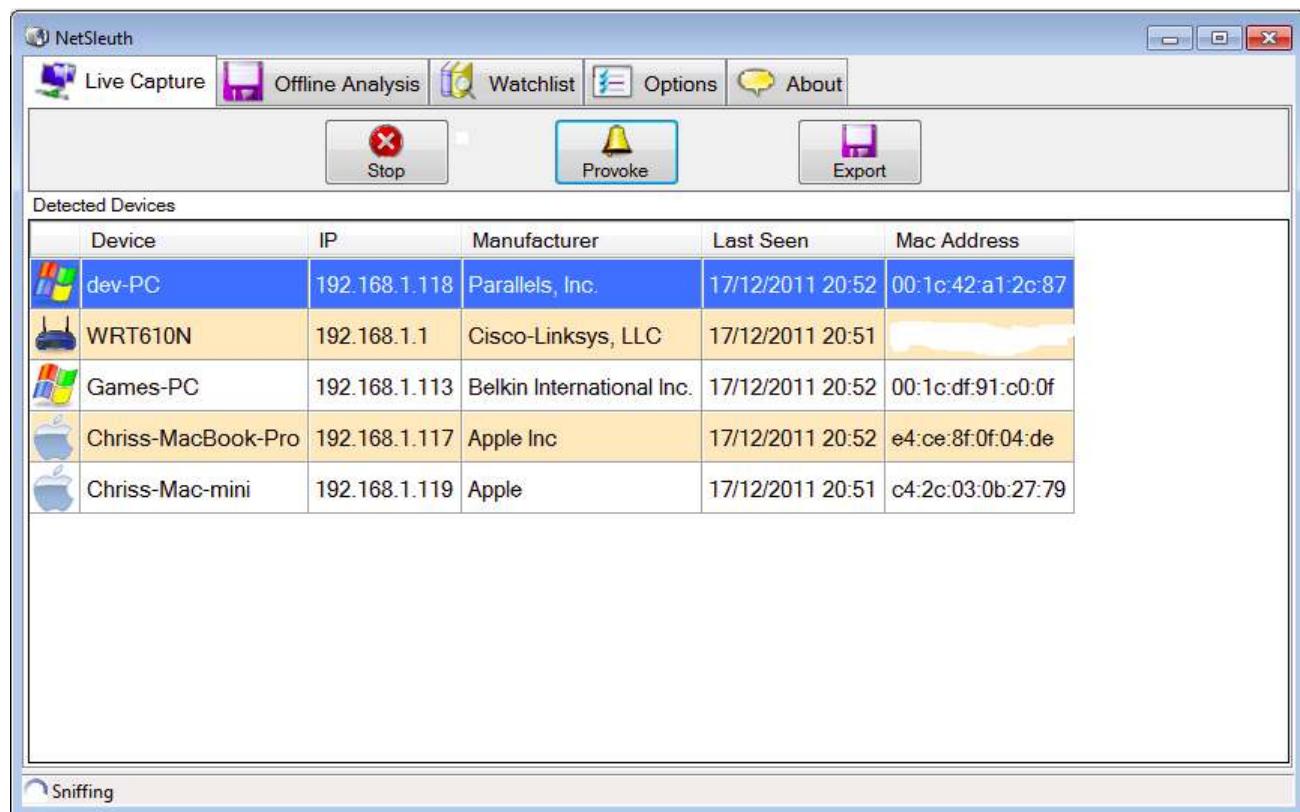
## 5.6) Outils Network Forensics

version : 06-10-2014 09:01

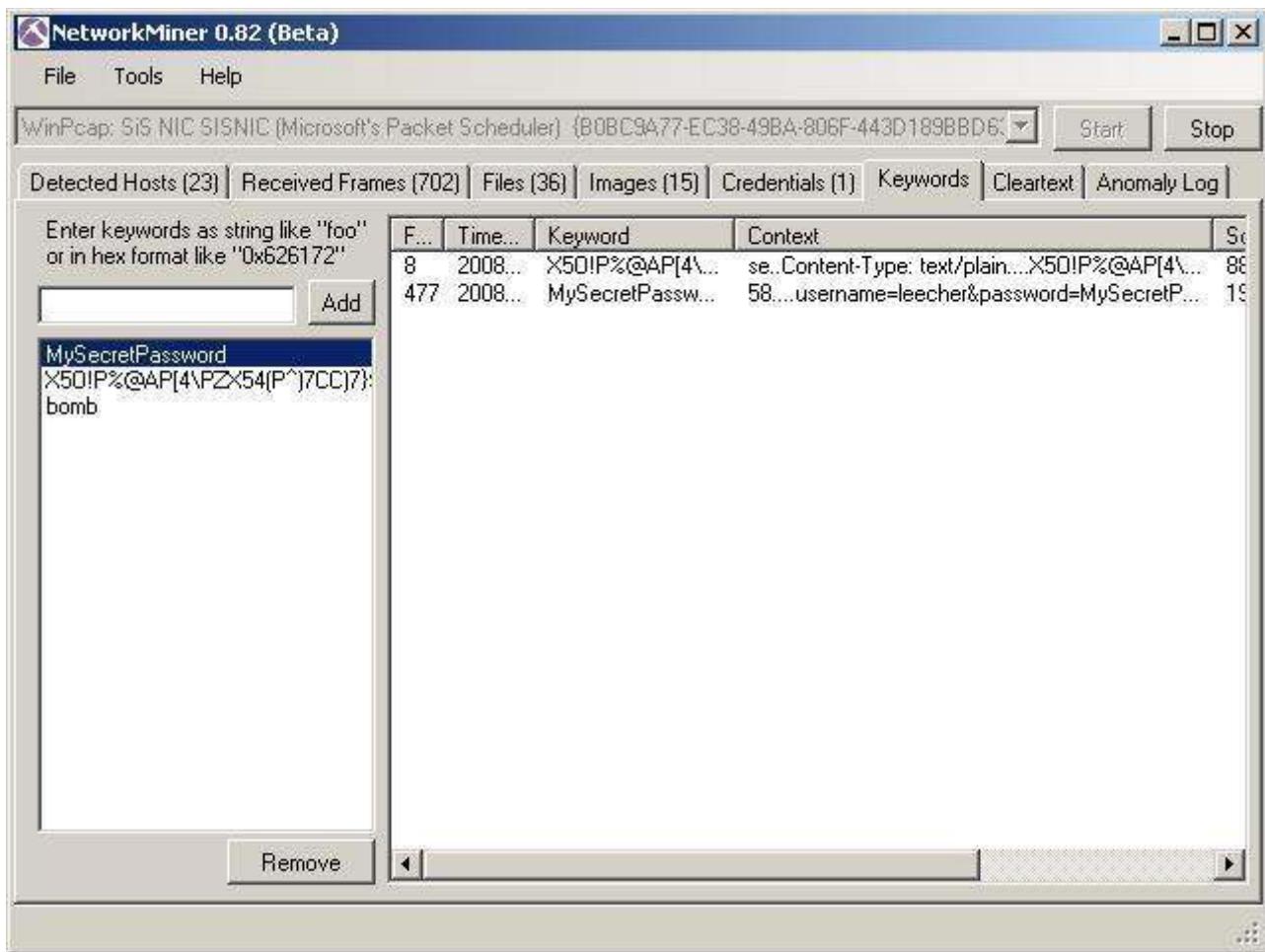
Quelques outils pour analyser les connexions réseau ou les paquets réseau :

- Wireshark : scanner réseau passif
- NetSleuth : scanner réseau passif
- NetworkMiner : extracteur de données sous Windows
- Argus : outil d'audit de la couche 2 et + du réseau
- Xplico : extracteur de données
- TCPDump : scanner réseau passif
- NTop : scanner réseau passif

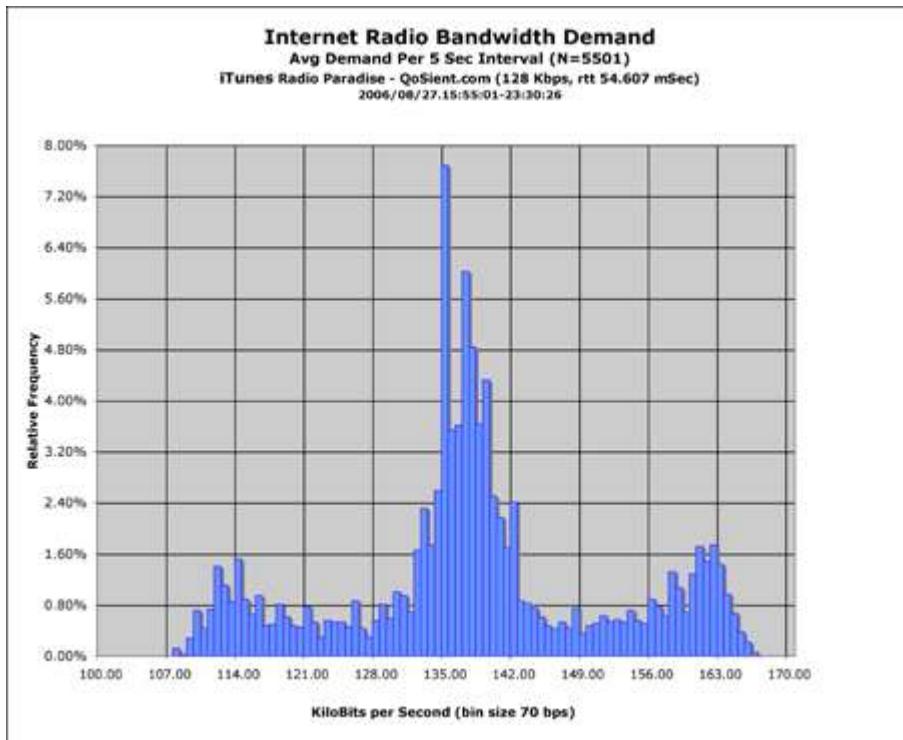
### NetSleuth



## NetworkMiner



## Argus



# Xplico

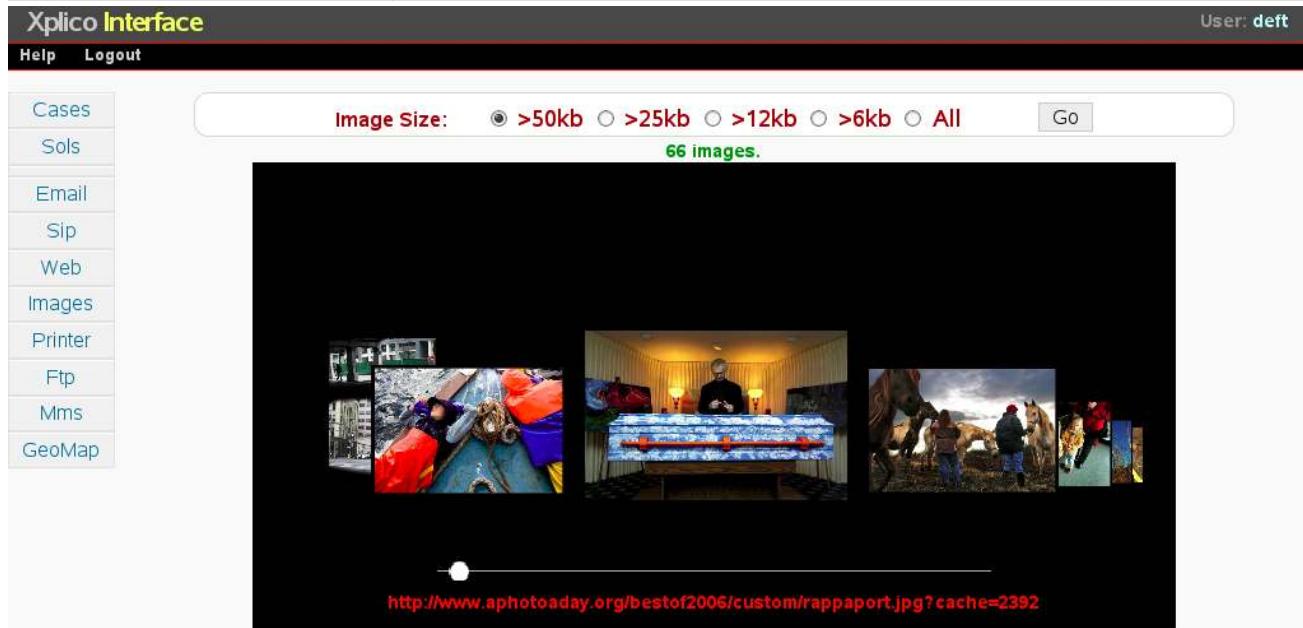
**Xplico Interface** User: deft

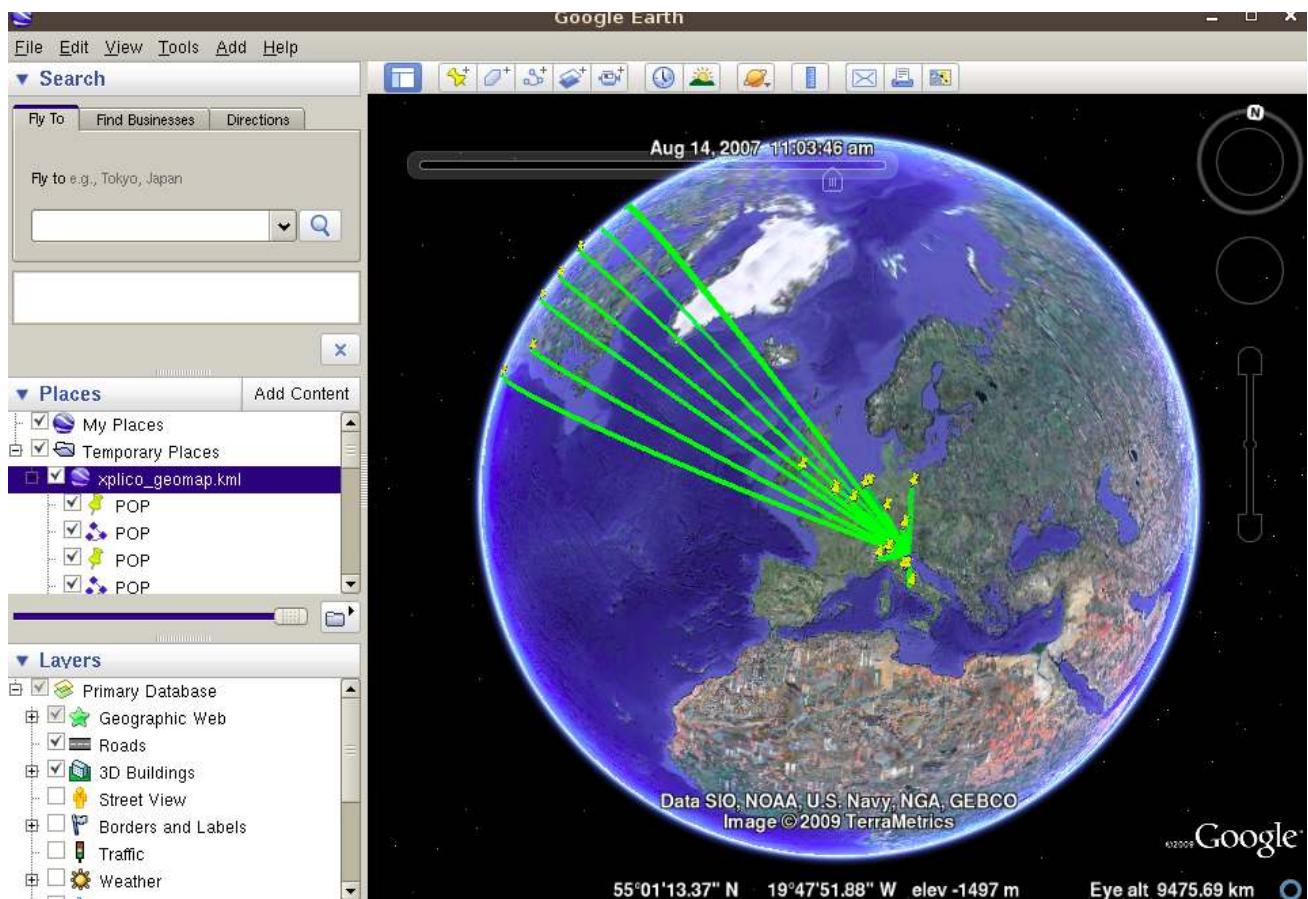
Help Logout

For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs:  Html  Image  Flash  Video  Audio  All Go

Date	Url	Size	Method	Info
2007-08-14 11:13:58	<a href="http://www.google.it/">www.google.it/</a>	1521	GET	info.xml
2007-08-14 11:13:33	<a href="http://track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&amp;t=1&amp;u=http%3A//www.aphotoaday.org/">track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&amp;t=1&amp;u=http%3A//www.aphotoaday.org/</a>	105	GET	info.xml
2007-08-14 11:13:22	<a href="http://track3.mybloglog.com/js/jsserv.php?mbID=2007011710424247">track3.mybloglog.com/js/jsserv.php?mbID=2007011710424247</a>	5276	GET	info.xml
2007-08-14 11:13:25	<a href="http://track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&amp;t=1&amp;u=http%3A//www.aphotoaday.org/">track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&amp;t=1&amp;u=http%3A//www.aphotoaday.org/</a>	105	GET	info.xml
2007-08-14 11:13:24	<a href="http://track3.mybloglog.com/js/jsserv.php?mbID=2007011710424247">track3.mybloglog.com/js/jsserv.php?mbID=2007011710424247</a>	5274	GET	info.xml
2007-08-14 11:13:23	<a href="http://rcm.amazon.com/e/cm?t=ap06-20&amp;o=1&amp;p=20&amp;l=qs1&amp;f=ifr">rcm.amazon.com/e/cm?t=ap06-20&amp;o=1&amp;p=20&amp;l=qs1&amp;f=ifr</a>	2669	GET	info.xml
2007-08-14 11:13:10	<a href="http://rcm.amazon.com/e/cm?t=ap06-20&amp;o=1&amp;p=20&amp;l=qs1&amp;f=ifr">rcm.amazon.com/e/cm?t=ap06-20&amp;o=1&amp;p=20&amp;l=qs1&amp;f=ifr</a>	2669	GET	info.xml
2007-08-14 11:13:04	<a href="http://www.aphotoaday.org/fronts.html">www.aphotoaday.org/fronts.html</a>	850	GET	info.xml
2007-08-14 11:13:37	<a href="http://www.aphotoaday.org/apadnews/">www.aphotoaday.org/apadnews/</a>	3793	GET	info.xml
2007-08-14 11:12:26	<a href="http://c14.statcounter.com/text.php?sc_project=1435373&amp;resolution=1280&amp;camefrom=http%3A//www.aphotoaday.org/">c14.statcounter.com/text.php?sc_project=1435373&amp;resolution=1280&amp;camefrom=http%3A//www.aphotoaday.org/</a>	25	GET	info.xml
2007-08-14 11:12:23	<a href="http://www.aphotoaday.org/favicon.ico">www.aphotoaday.org/favicon.ico</a>	320	GET	info.xml
2007-08-14 11:12:08	<a href="http://www.aphotoaday.org/favicon.ico">www.aphotoaday.org/favicon.ico</a>	320	GET	info.xml
2007-08-14 11:12:08	<a href="http://www.aladingenius.com/theMagicLamp/">www.aladingenius.com/theMagicLamp/</a>	6775	GET	info.xml
2007-08-14 11:12:07	<a href="http://www.aphotoaday.org/bestof2006/">www.aphotoaday.org/bestof2006/</a>	604	GET	info.xml
2007-08-14 11:12:07	<a href="http://www.aphotoaday.org/">www.aphotoaday.org/</a>	1390	GET	info.xml
2007-08-14 11:12:02	<a href="http://www.photoblogdirectory.org/buttons/photoblogdirectory_bw.gif">www.photoblogdirectory.org/buttons/photoblogdirectory_bw.gif</a>	1606	GET	info.xml
2007-08-14 11:11:52	<a href="http://www.aladingenius.com/templates/themagiclamp_2006/img/back.gif">www.aladingenius.com/templates/themagiclamp_2006/img/back.gif</a>	238	GET	info.xml
2007-08-14 11:11:51	<a href="http://www.aladingenius.com/templates/themagiclamp/index.php?x=browse&amp;pageNum=1">www.aladingenius.com/templates/themagiclamp/index.php?x=browse&amp;pageNum=1</a>	14029	GET	info.xml
2007-08-14 11:11:47	<a href="http://www.aladingenius.com/templates/themagiclamp_2006/img/back.gif">www.aladingenius.com/templates/themagiclamp_2006/img/back.gif</a>	238	GET	info.xml
2007-08-14 11:11:42	<a href="http://www.aladingenius.com/favicon.ico">www.aladingenius.com/favicon.ico</a>	209	GET	info.xml





## 5.7) Outils Social Forensics

version : 06-10-2014 09:01

- Pas de logiciel dédié à cela
- Recherche à la "mano"
- ou par des outils de "Data mining"
- ou "d'Intelligence économique"