

Analyse forensique du cloud en RAM

N. SCHERRMANN - P. VEUTIN

23 janvier 2017 - CoRI&IN 2017



>_ Présentations

- N. Scherrmann
 - Ingénieur R&D @ TRACIP
- P. Veutin
 - Responsable R&D @ TRACIP
- TRACIP

>_ Sommaire

- Enjeux
- Rappels CoRI&IN 2016
- TRACIP DAY
- Ajouts

>_ Enjeux

Pourquoi s'intéresser à la RAM ?

- peu traitée en forensic
- masse de données
- données utilisateur/applications/OS

Pourquoi s'intéresser au Cloud ?

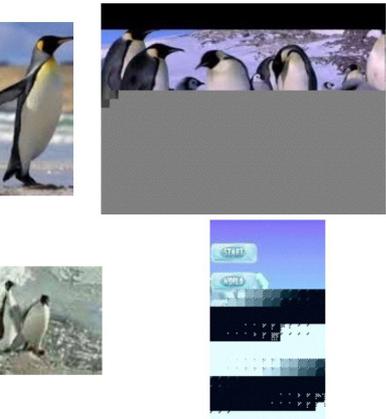
- peu traité en forensic
- freins/blocages juridiques
- démocratisation
- le futur ?!

Pourquoi s'intéresser à l'analyse des données du Cloud en RAM ?

- pour toutes ces raisons

>_ Rappels - CoRI&IN 2016

- Nécessité de remapper la mémoire vive
- De nombreuses traces uniquement en mémoire
- Outils DF pas adaptés / pas exhaustif
- Outils IR pas adaptés pour DF
- Développement d'un outil dédié



Outils	# fichiers	Pingouin
IEF	469	<i>non</i>
EnCase 7	478	<i>non</i>
X-Ways	510	
FTK	519	
APF	593	
scalpel	520	



Outils	# fichiers	Pingouin
IEF	116	<i>oui</i>
EnCase 7	119	<i>oui</i>
X-Ways	120	<i>oui</i>
FTK	121	<i>oui</i>
APF +	118	<i>oui</i>
scalpel	119	<i>oui</i>

>_ Rappels CoRI&IN 2016

- Récupération d'informations de Gmail en RAM
 - Sujets de mail (même non-lus, non-affichés)
 - Adresses mail (contacts, même non-connues)
 - Hangouts



>_ Le saviez-vous #1

Google (entre autres) autorise (conformément à la RFC 5233) l'utilisation des tags

toto+TAG@gmail.com

Il faut donc autoriser le caractère '+' dans la partie locale (partie située avant le @) des adresses mail.

Attention d'autres caractères '+' peuvent être présents avant le tag ...

toto+tata+TAG@gmail.com

... Pensez à mettre à jour vos expressions régulières ...

>_ Le saviez-vous #2

Google autorise l'ajout des points '.' entre chaque caractère dans une adresse mail.

Ainsi des mails envoyés à

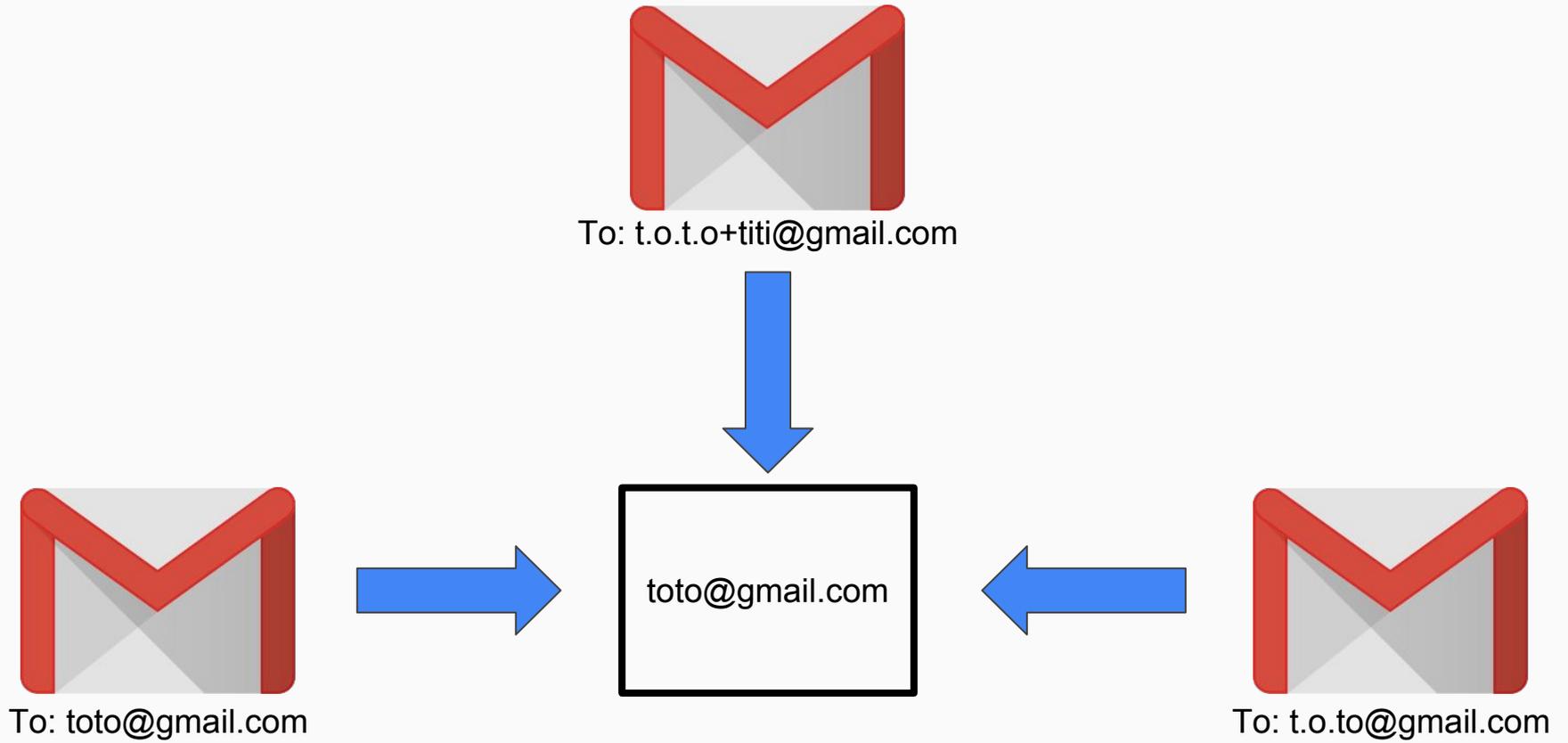
toto@gmail.com

ou à

t.o.t.o@gmail.com

arriveront dans la même boîte Gmail.

>_ Pour faire simple



>_ Le rapport ?

Corrélation des données retrouvées :

toto@gmail.com = t.o.t.o@gmail.com = t.o.to+tata15241@gmail.com

Google fait automatiquement le lien (parfois)

```
[  
  "nicoscherrmann@gmail.com",  
  "nico.scherrmann@gmail.com",  
  "nscherrmann@tracip.fr",  
  "n.i.c.o.s.c.h.e.r.r.m.a.n.n@gmail.com"  
]
```

En investigation numérique, il est indispensable de faire la part des choses ...

Mais

Google = 333 TM

Source : https://www.google.com/intl/fr_ALL/permissions/trademark/trademark-list.html le 16-01-17

>_ Autant de services ?

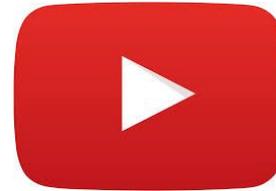
Traces en RAM non - traitées

Traces en RAM traitées

Google Search



Youtube



Google Maps



Google Agenda

GMail



Google Plus



Google Hangouts

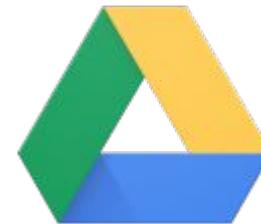


Google Drive



Google Docs

Google Fit



My Activity



Google Takeout

>_My Activity

Historique consultable & Exportable

The screenshot shows a web browser window with the address bar displaying "https://myactivity.google.com/myactivity?q=signal&product=1". The page content is organized into a left sidebar and a main activity list.

Left Sidebar:

- Retour
- Vue par groupe
- Vue par élément
- Supprimer des activités par
- Autre activité Google
- Commandes relatives à l'activité
- Mon compte
- Aide
- Envoyer des commentaires

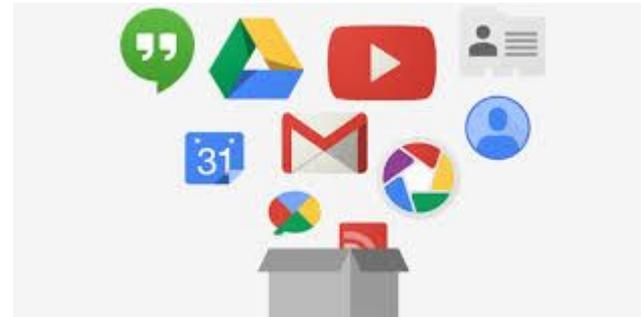
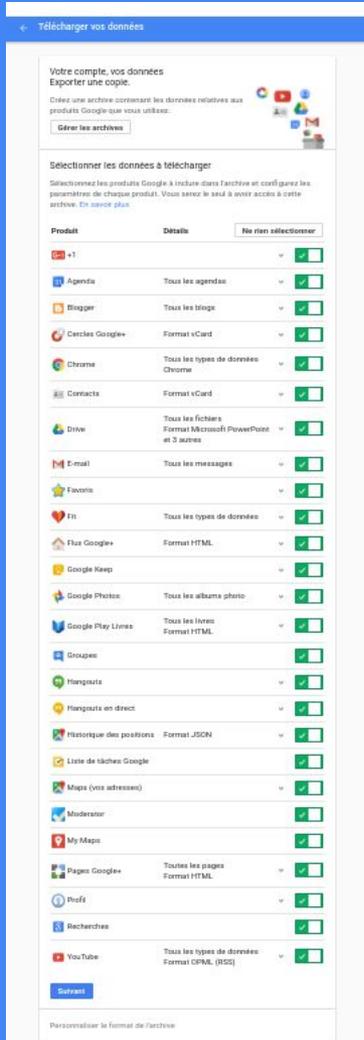
Main Activity List:

- 27 juin 2016** (22:07)
 - Signal Private Messenger
 - Application utilisée : [Signal Private Messenger](#)
 - Détails • [Signal Private Messenger](#)
 - Signal Private Messenger
 - Application utilisée : [Signal Private Messenger](#)
 - Détails • [Signal Private Messenger](#)
- 25 juin 2016** (20:42)
 - Signal Private Messenger
 - Application utilisée : [Signal Private Messenger](#)
 - Détails • [Signal Private Messenger](#)

Confidentialité • Conditions

>_Takeout

Un service pour les
gouverner sauvegarder
tous



Google Takeout / takeout.google.com

Toute une vie ? en quelques fichiers

Possibilité de télécharger toutes les infos dont dispose
Google sur nous.

Fichiers natifs / Fichiers propriétaires

Structure(s) JSON

Pratique pour identifier des structures (ID, URLs, ...)

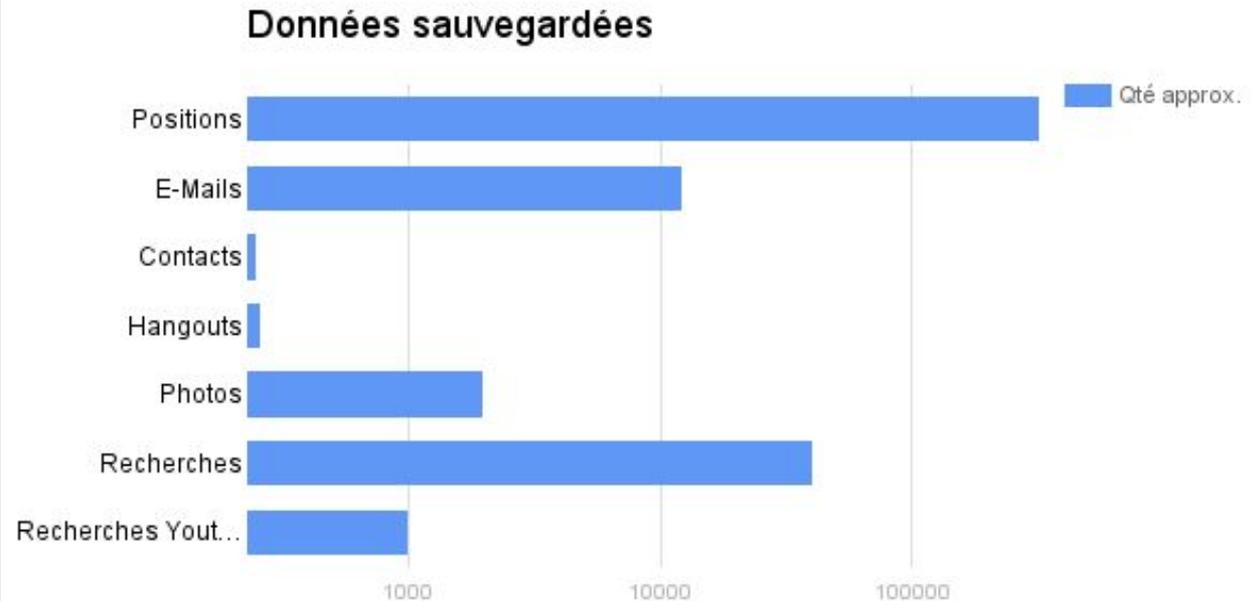
>_Takeout sur Compte perso

Utilisation “standard”

- 0 tracker d'activité
- 1 GSM Android
- déconnexion dès que possible/j'y pense
- Google principal SE
- boîte “perso” GMail
- peu de hangouts
- très peu de G+

Au total **10,3 Go** de données réparties sur ~ 20 ans

(les services ayant été activés au fur et à mesure, le volume de données tend à croître les dernières années).



>_ Rappels TRACIP DAY

- Suite des travaux sur la RAM :

- Google Drive

- Récupération des fichiers
 - Récupération des informations sur les fichiers



- Google Docs

- Récupération des métadonnées
 - Récupération du document



- **Récupération et rejeu de la saisie**

➤ Démonstration

Récupération de la saisie dans Google Docs

>_ Démonstration

```
schermi@darkknightMB ~/Documents/Python/CORIN2K17
```

>_ Suite des recherches

Récupération des commentaires

Récupération des images de profils des participants

Analyse des sauvegardes automatiques

Comparaison avec la saisie récupérée

Utilisation détournée de Google Docs

>_ Édition collaborative

The screenshot shows a Google Docs interface for a document titled "CORI&IN 2K17". The document content is a numbered list:

- 1- Présentations
- 2- Contexte
- 3- Evaluation du besoin pour le ranch
- 4- Propositions de solutions

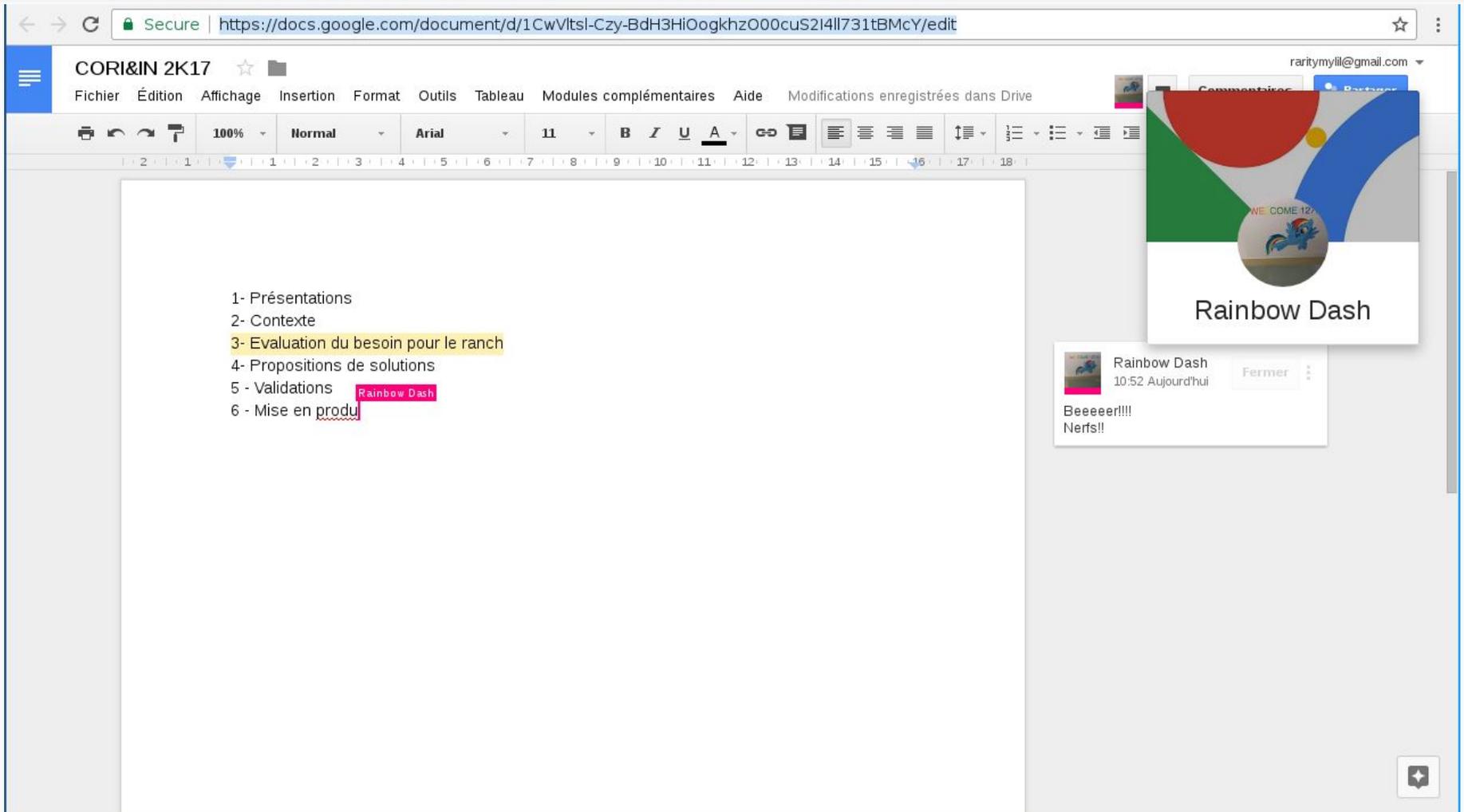
A comment from "Rainbow Dash" is visible on the right side, dated "10:52 Aujourd'hui", with the text "Beeeeeer!!!!". The comment box includes a "Fermer" button.

The interface includes a top navigation bar with "Fichier", "Édition", "Affichage", "Insertion", "Format", "Outils", "Tableau", "Modules complémentaires", and "Aide". The status bar shows "Modifications enregistrées dans Drive". The document is being edited by "raritymylil@gmail.com".

>_ Edition collaborative

- Plusieurs utilisateurs peuvent éditer le document simultanément
- Utilisateurs “Google” : rw-
- Utilisateurs “externe” : r--
- Téléversement de fichiers Word ou Libreoffice
- Création de document directement depuis l’interface

>_ Traçabilité des modifications



The image shows a Google Docs interface with a document titled "CORI&IN 2K17". The document content is a list of six items:

- 1- Présentations
- 2- Contexte
- 3- Evaluation du besoin pour le ranch
- 4- Propositions de solutions
- 5 - Validations
- 6 - Mise en produ

A comment from "Rainbow Dash" is visible on the right side of the document, pointing to the word "produ" in item 6. The comment text is:

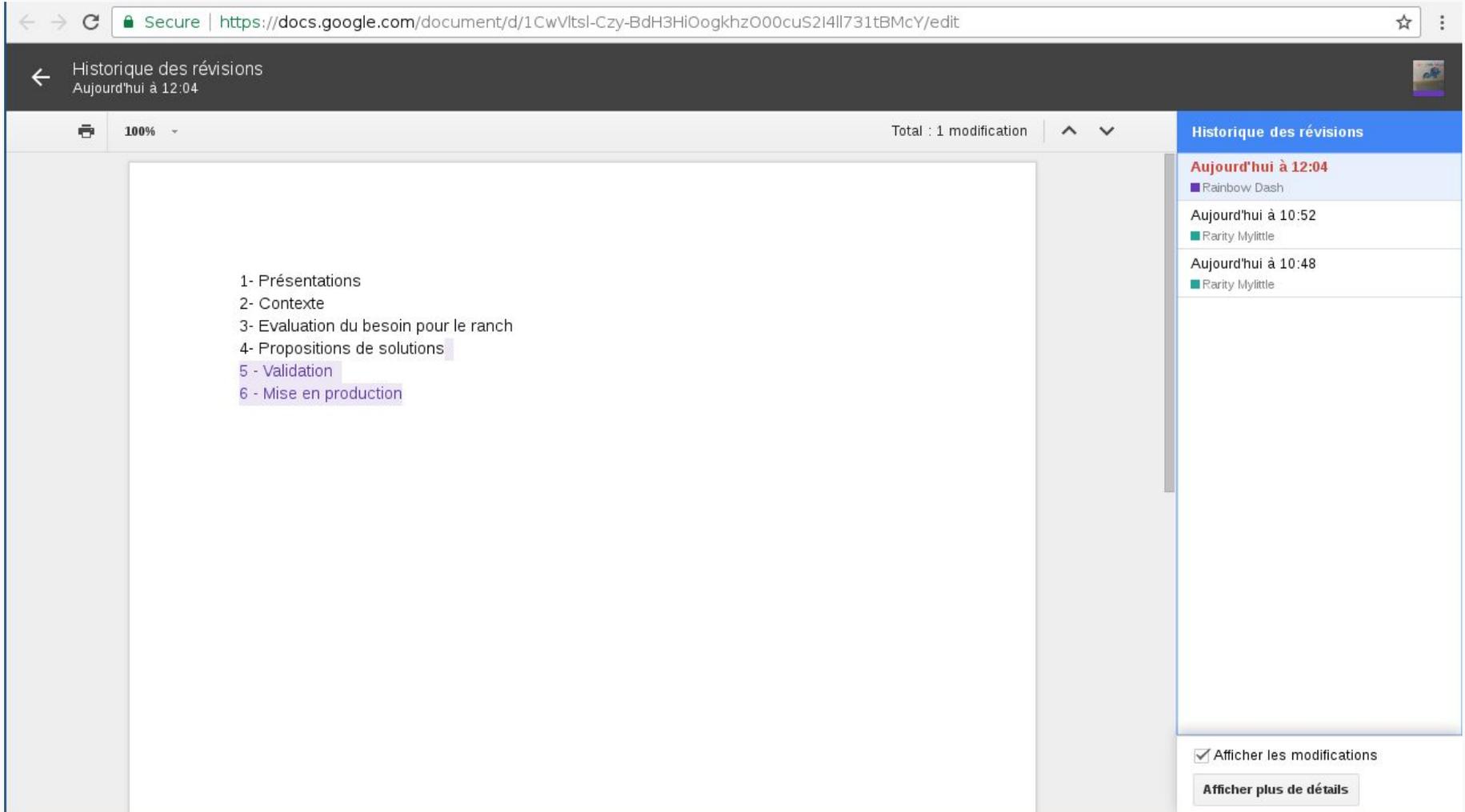
Beeeeer!!!
Nerfs!!

The comment is displayed in a white box with a profile picture of Rainbow Dash and a "Fermer" button. The document's toolbar and navigation elements are also visible at the top.

>_ Traçabilité des modifications

- Visualisation des utilisateurs pouvant éditant et leur statut de connexion
- Visualisation de la position du curseur des utilisateurs et du texte tapé/effacé

>_ Historique des modifications



The screenshot shows a Google Docs document titled "Historique des révisions" (Revision History) with a timestamp of "Aujourd'hui à 12:04". The document content is a numbered list of six items:

- 1- Présentations
- 2- Contexte
- 3- Evaluation du besoin pour le ranch
- 4- Propositions de solutions
- 5 - Validation
- 6 - Mise en production

The right sidebar contains a "Historique des révisions" (Revision History) panel. It lists three revisions:

- Aujourd'hui à 12:04** (Rainbow Dash)
- Aujourd'hui à 10:52 (Rarity Mylittie)
- Aujourd'hui à 10:48 (Rarity Mylittie)

At the bottom of the sidebar, there is a checkbox labeled "Afficher les modifications" (Show changes) which is checked, and a button labeled "Afficher plus de détails" (Show more details).

>_ Historique des modifications

- Génération de versions du document
- Visualisation des modifications apportées au document ainsi que leurs auteurs
- Restauration à des versions antérieures

>_ Sauvegarde automatique

- Sauvegarde automatique du document
- Génération automatique des révisions
- Entre deux révisions seuls les éléments ajoutés sont enregistrés, si du texte ajouté est supprimé, la suppression n'est pas stockée.

>_ **Démonstration**

Sauvegarde auto

>_ Commentaires

The screenshot shows a Google Docs interface. The document title is "CORI&IN 2K17". The main content area contains a numbered list and two paragraphs of placeholder text. The comment thread on the right includes:

- Comment 1:** User: Rainbow Dash, Time: 10:52 16 janv., Content: "Beeeeeer!!! Nerfs!!", Action: Fermer
- Comment 2:** User: Rarity Mylittle, Time: 16:05 17 janv., Content: "Philippe?", Action: Fermer
- Comment 3:** User: Rainbow Dash, Time: 16:01 17 janv., Content: "Controut", Action: Fermer
- Comment 4:** User: Rainbow Dash, Time: 16:02 17 janv., Content: "super anonymisation double flux, c'est comme pour les pots d'échappement ... ou les clim", Action: Fermer
- Comment 5:** User: Rainbow Dash, Time: 16:46 16 janv., Content: "Supprimer : 'usto'", Action: Fermer

>_ Commentaires

- 2 types de commentaires :
 - Commentaires du document
 - Suggestions de modification sur le texte

The screenshot shows a Google Docs interface for a document titled "CORI&N 2K17". The document content includes a numbered list of sections and two paragraphs of placeholder text. A chat window is overlaid on the right side of the document, showing a conversation between "Rainbow Dash" and "Rarity Mylittl". The chat messages are:

- Rainbow Dash (10:52 16 janv.): Beeeer!!!! Nerfs!!
- Rarity Mylittl (16:05): Philippe?
- Rainbow Dash (16:01): Coucou moi yop
- Rainbow Dash (16:02): super anonym comme pour ... ou les clim

The chat window also shows a search bar with "(2) Rainbow Dash,Rarity Mylittl" and a settings gear icon.

>_ Chat

- Chat intégré directement dans l'interface pour communiquer sur le document
- Ressource différente de Hangout

>_ Résumé des ressources disponibles

- Edition collaborative
- Identifications des auteurs
- Malgré la sauvegarde automatique, toutes les saisies ne sont pas enregistrées

- **Il est possible d'utiliser Google Docs en tant que messagerie instantanée sans sauvegarde de l'historique**

>_ Démonstration

Détournement de Google Docs en Cover Chat

>_ Structures du navigateur retrouvées en mémoire

- Informations du compte
- Informations du document
- Commentaires du document
- Messages du chat
- Participants du chat
- Texte de l'édition





>_ Commentaires

```
schermi@darkknightMB ~/Documents/Python/CORIN2K17 python demo.py -f /home/schermi/Documents/Confs/CORIN2K17/commentaires.dmp.13549 -  
m commentaire
```





>_ Edition utilisateur

```
schermi@darkknightMB ~/Documents/Python/CORIN2K17
```

>_ Edition participant

```
schermi@darkknightMB ~/Documents/Python/CORIN2K17
```

>_ Pour aller plus loin

- Les informations récupérées lors de l'édition ne permettent pas encore de reconstruire entièrement le document
- Il est possible de récupérer les images de profils directement en RAM mais nous n'avons pas encore trouvé de lien avec les profils Google
- Les informations du documents ne permettent pas pour le moment d'identifier les personnes y ayant accès

>_ QUESTIONS ?

(BB)?

William Shakespeare