Analyse forensique du cloud en RAM

N. SCHERRMANN - P. VEUTIN

23 janvier 2017 - CoRI&IN 2017

TRACIP
Technologies & Services d'Investigation

>_ Présentations

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

TRACIP
Technologies & Services d'Investigation

>_ Sommaire

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

TRACIP
Technologies & Services d'Investigation

>_ 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 ?!

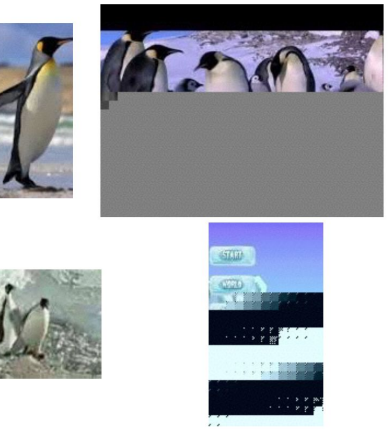
Pourquoi s'intéresser à l'analyse des données du Cloud en RAM ?

- 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	*non*
EnCase 7	478	*non*
X-Ways	510	
FTK	519	
APF	593	
scalpel	520	

Outils	# fichiers	Pingo
IEF	116	*oui*
EnCase 7	119	*oui*
X-Ways	120	*oui*
FTK	121	*oui*
APF †	118	*oui*
scalpel	119	*oui*

TRACIP
Technologies & Services d'Investigation

>_ 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

TRACIP
Technologies & Services d'Investigation

>_ 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

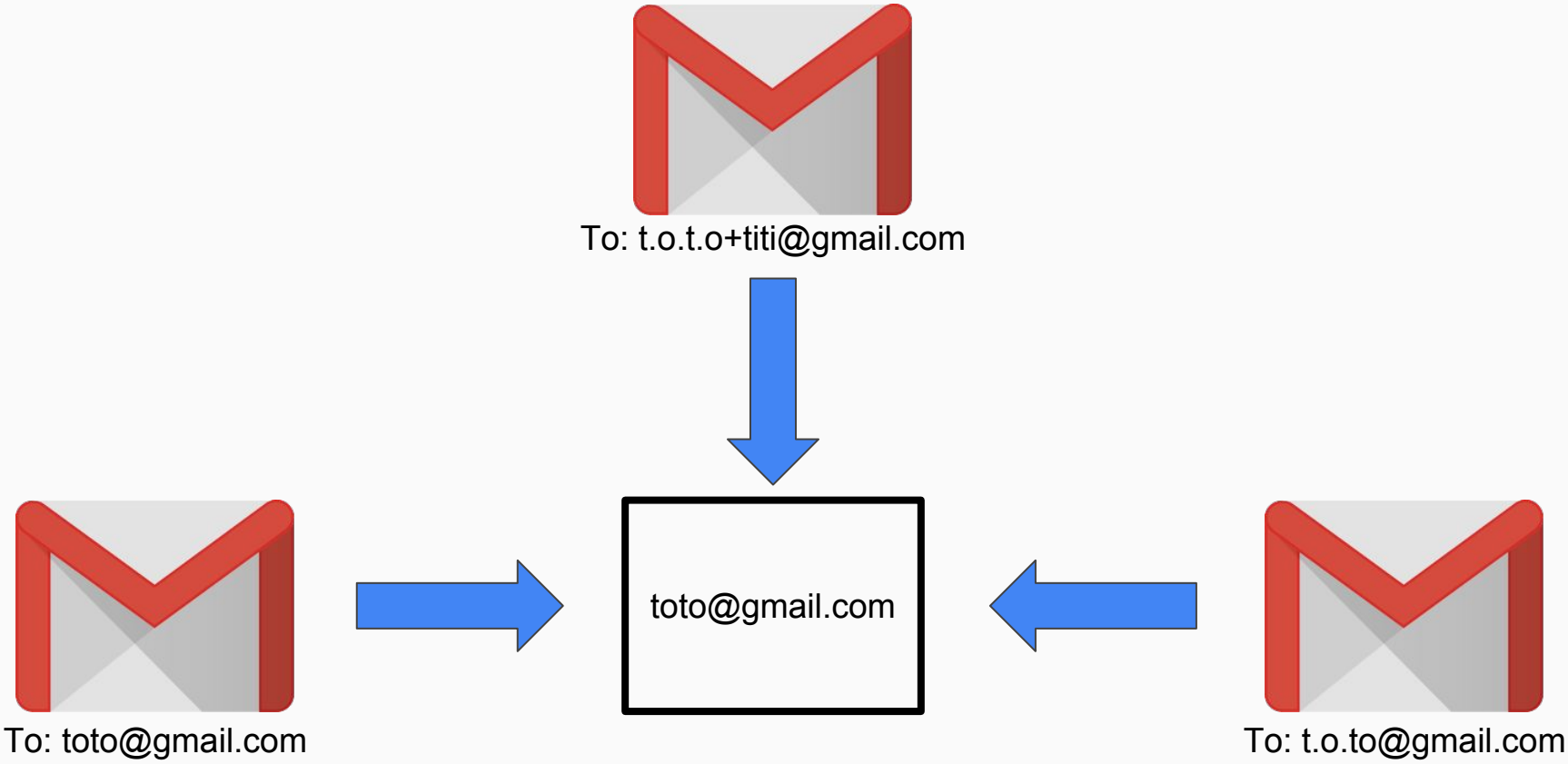
toto@gmail.com

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 ™

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

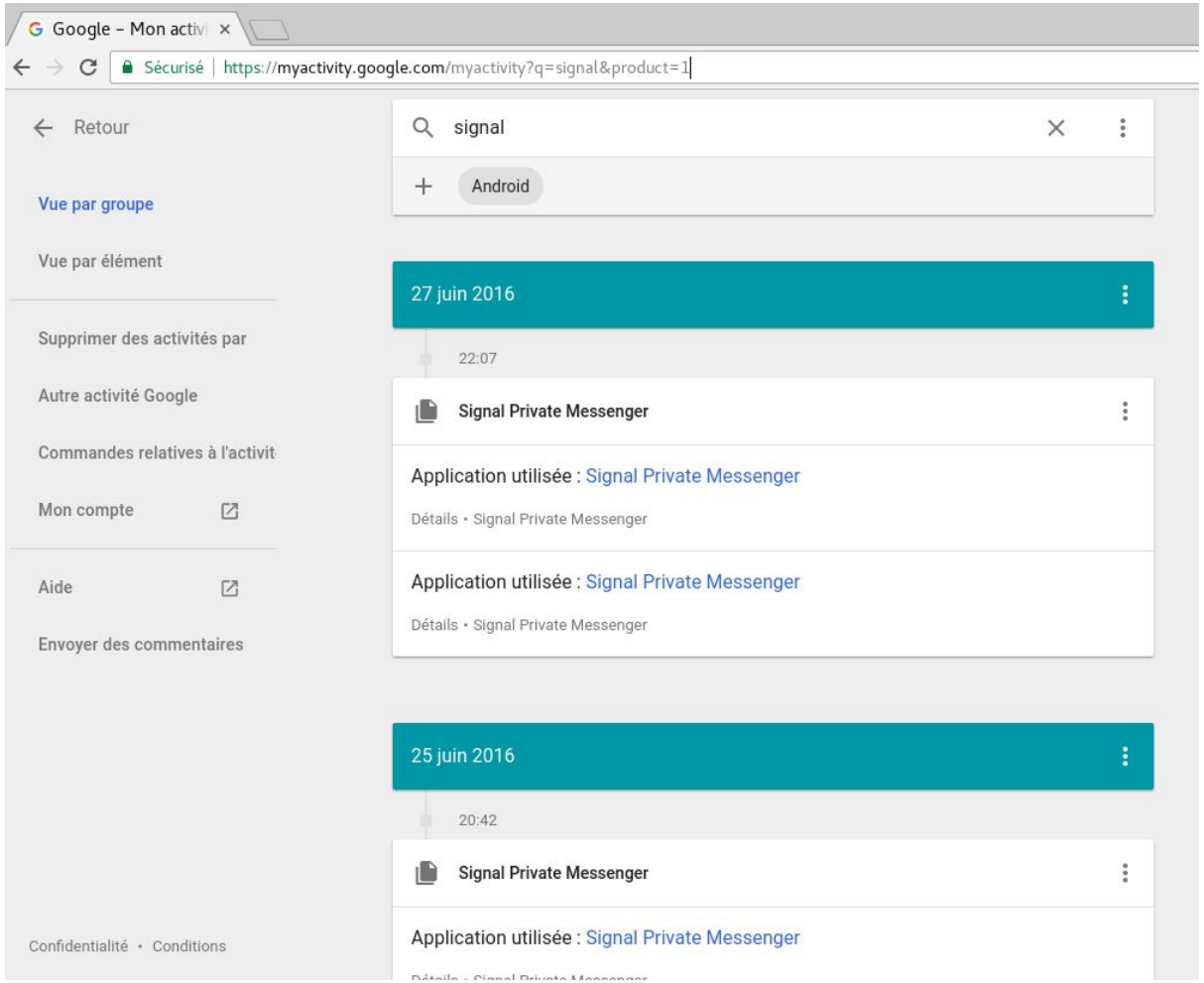
☐ Google Fit

☐ My Activity

☐ Google Takeout

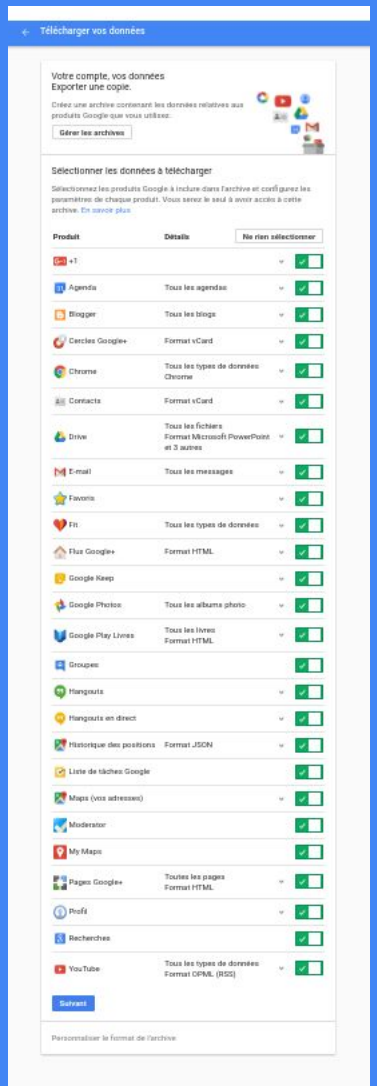
>_My Activity

Historique consultable & Exportable



>_Taketout

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

<u>Pratique pour identifier des structures (ID, URLs, …)</u>

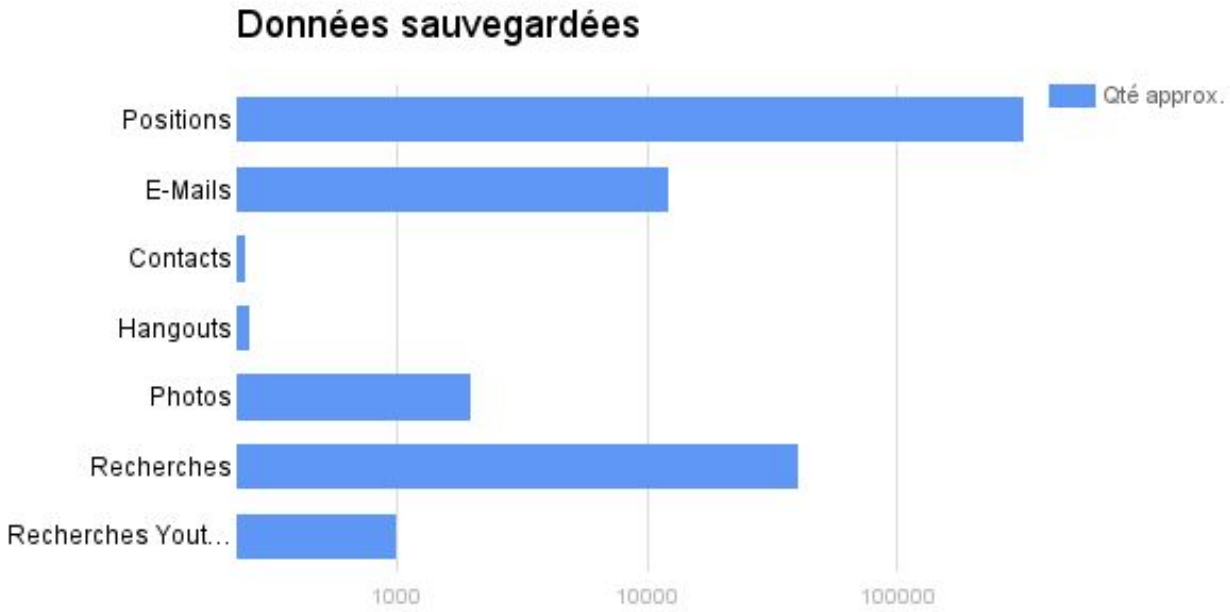
>_Takeout sur Compte perso

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

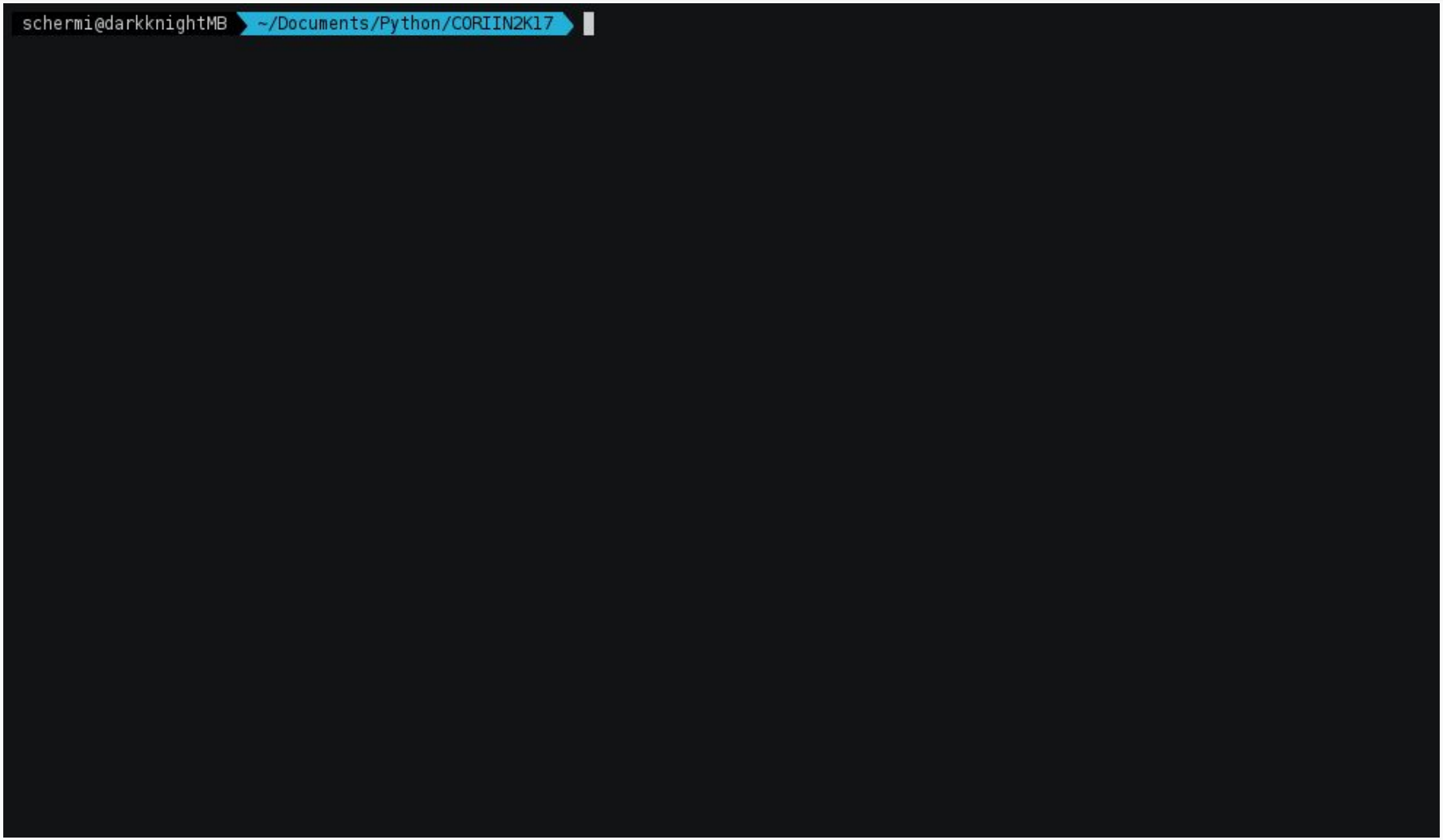
    - **Récupération et rejeu de la saisie**

TRACIP
Technologies & Services d'Investigation

>_ Démonstration

Récupération de la saisie dans Google Docs

>_ Démonstration



TRACIP
Technologies & Services d'Investigation

>_ Suite des recherches

Récupération des commentaires

Récupération des images de profils des participants

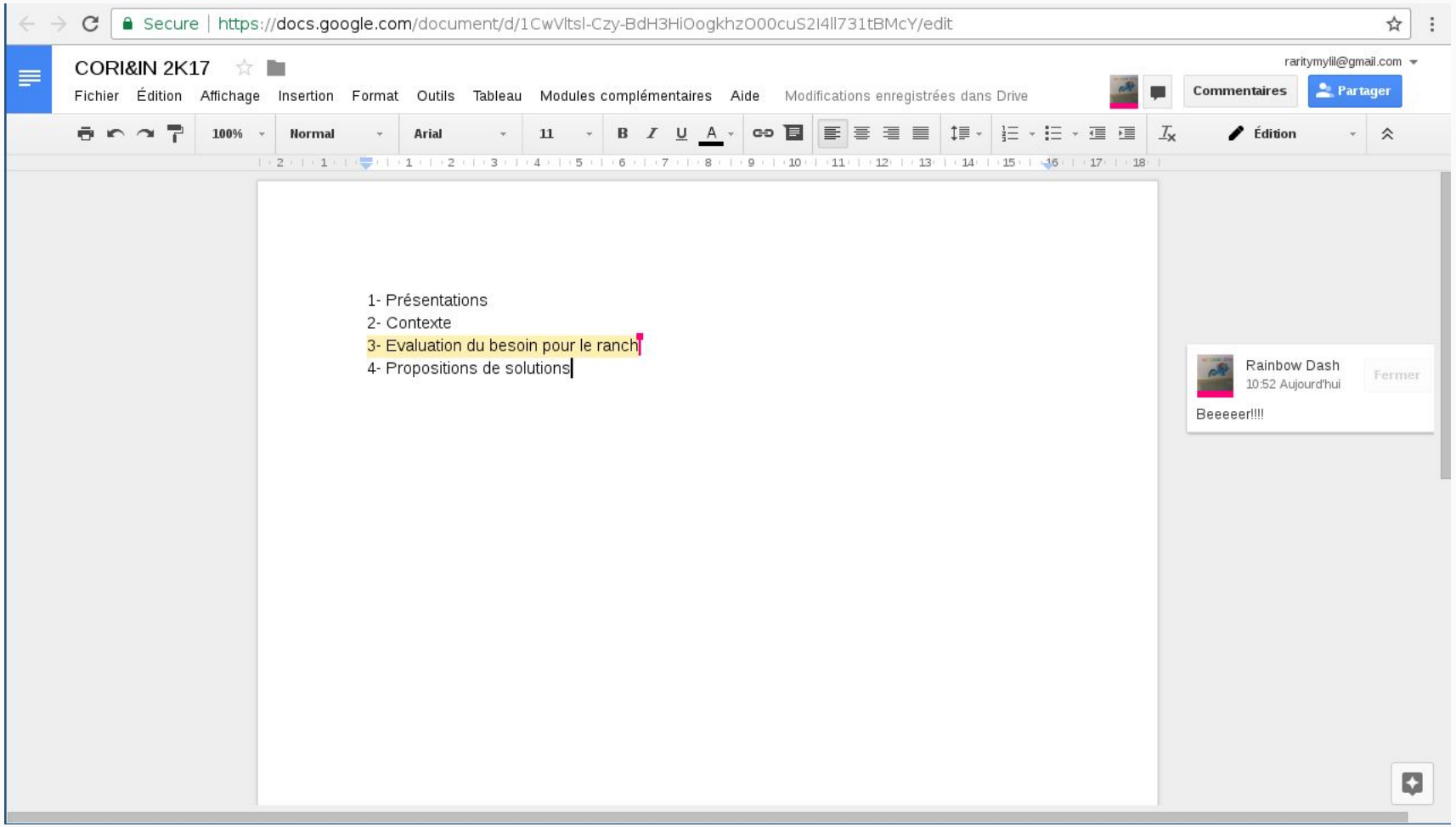
Analyse des sauvegardes automatiques

Comparaison avec la saisie récupérée

Utilisation détournée de Google Docs

TRACIP
Technologies & Services d'Investigation

>_ Édition collaborative



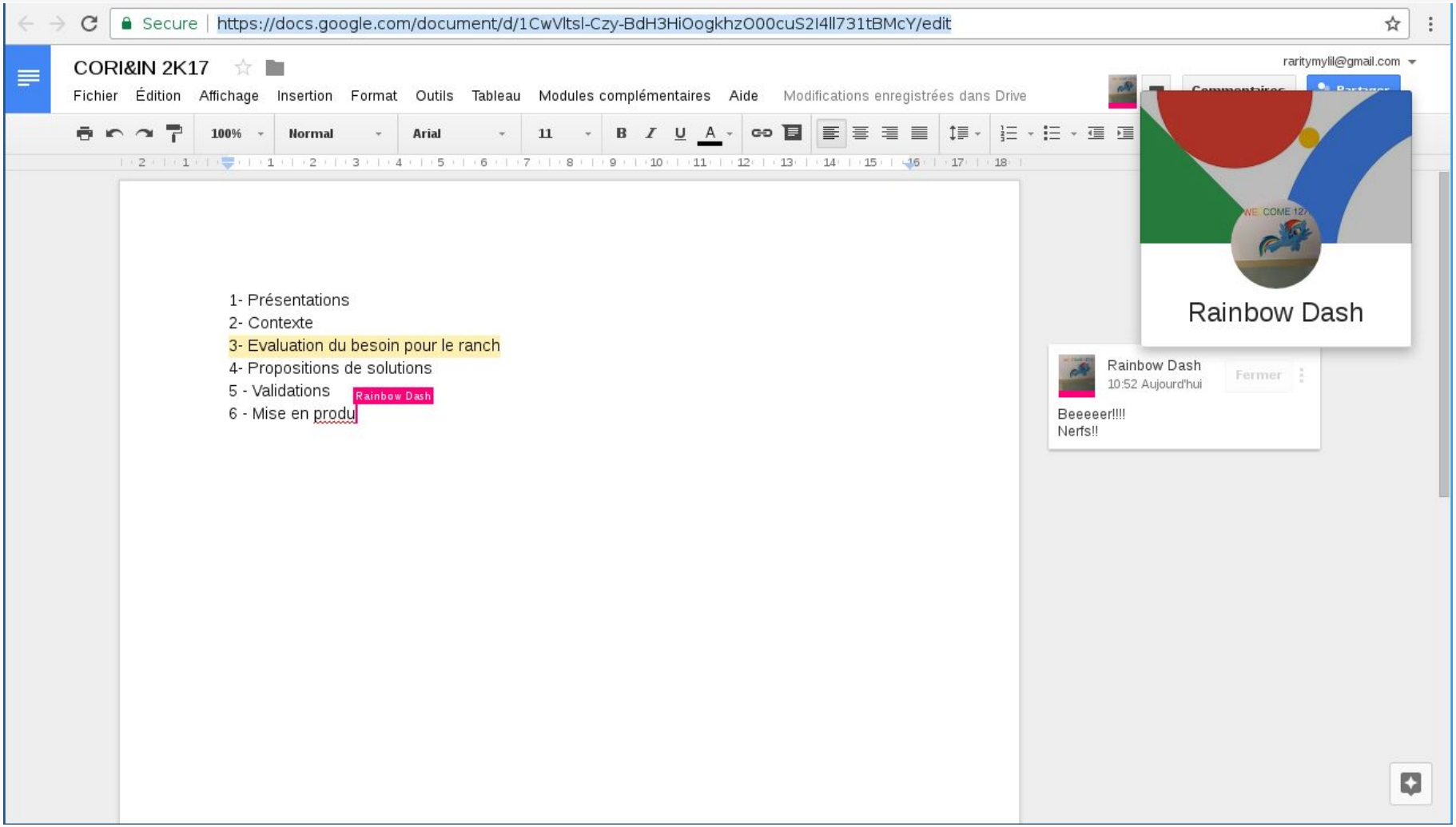
TRACIP
Technologies & Services d'Investigation

>_ 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

TRACIP
Technologies & Services d’Investigation

>_ Traçabilité des modifications



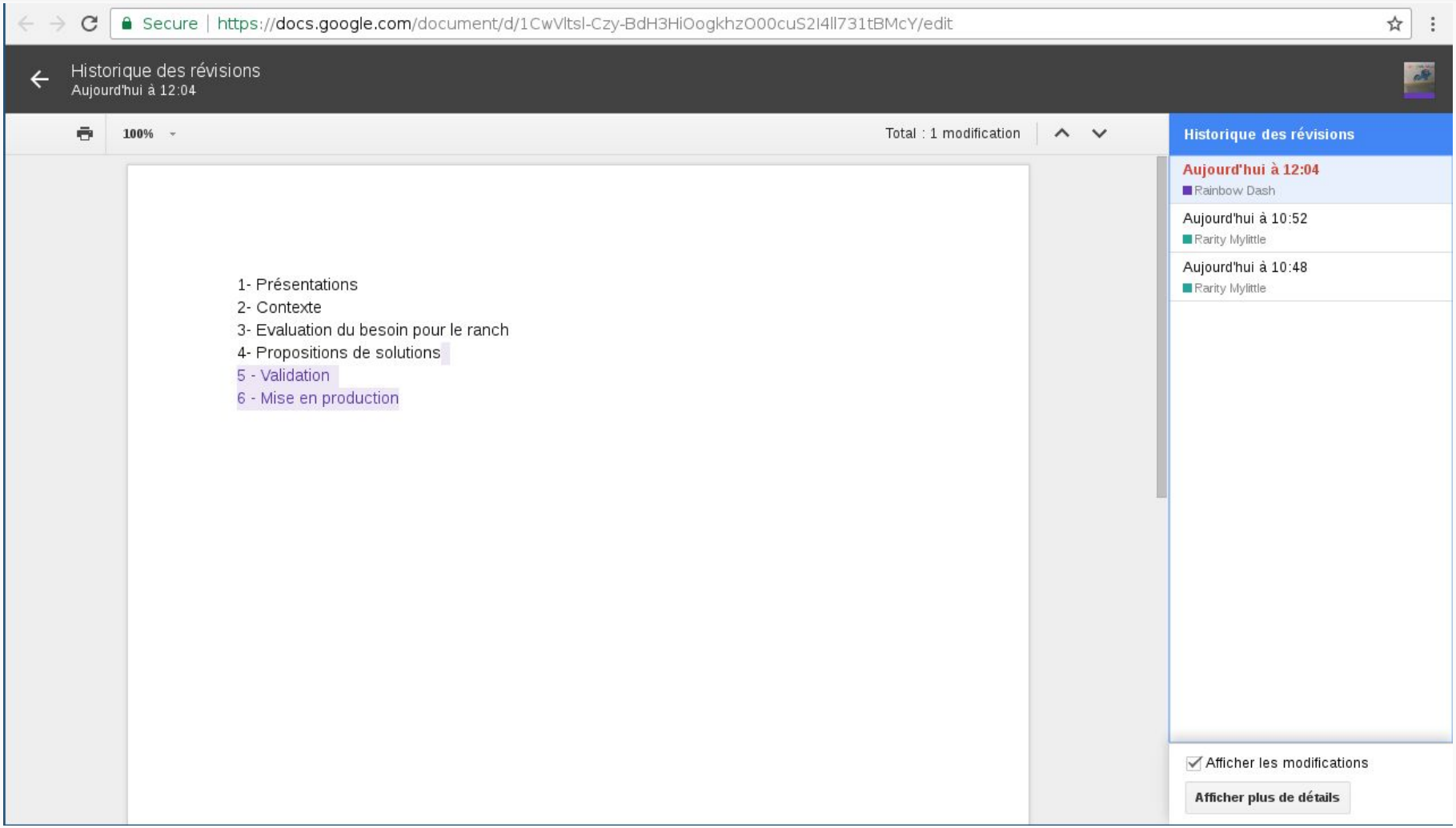
TRACIP
Technologies & Services d'Investigation

>_ 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

TRACIP
Technologies & Services d'Investigation

>_ Historique des modifications



TRACIP
Technologies & Services d'Investigation

>_ Historique des modifications

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

TRACIP
Technologies & Services d'Investigation

>_ Sauvegarde automatique

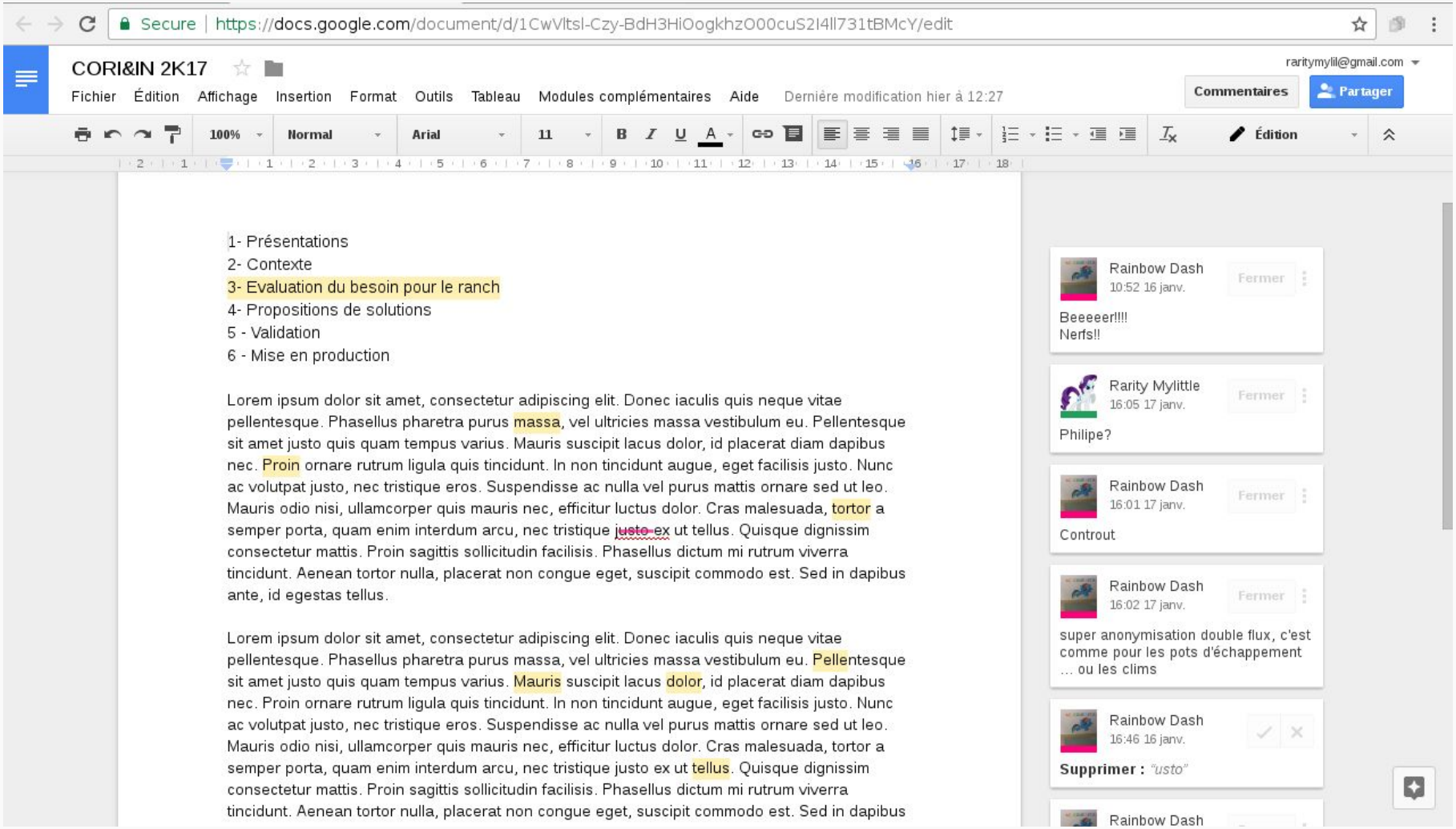
- Sauvegarde automatique du document
- Génération automatique des révisions
- Entre deux révisions seuls les éléments ajoutés sont enregistrés, si du texte ajouté est supprimé, la suppression n'est pas stockée.

TRACIP
Technologies & Services d'Investigation

>_ Démonstration

Sauvegarde auto

>_ Commentaires



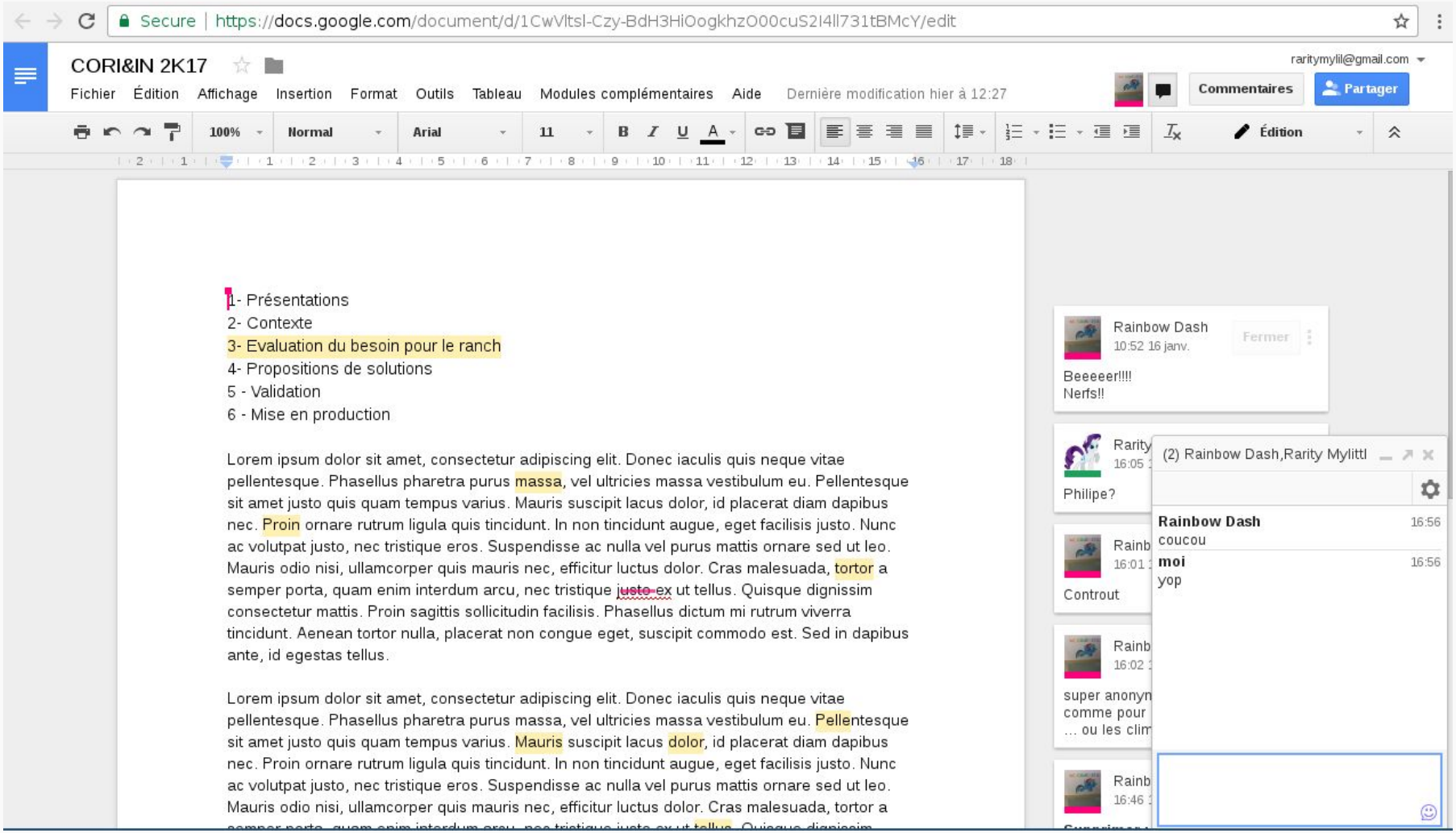
TRACIP
Technologies & Services d'Investigation

>_ Commentaires

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

TRACIP
Technologies & Services d'Investigation

>_ Chat



TRACIP
Technologies & Services d'Investigation

>_ Chat

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

TRACIP
Technologies & Services d'Investigation

>_ 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**

TRACIP
Technologies & Services d'Investigation

>_ 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

TRACIP
Technologies & Services d’Investigation

>_ Informations du compte

TRACIP
Technologies & Services d'Investigation

>_ Informations du document

TRACIP
Technologies & Services d'Investigation

>_ Commentaires

```
schermi@darkknightMB ~/Documents/Python/CORIIN2K17 python demo.py -f /home/schermi/Documents/Confs/CORIIN2K17/commentaires.dmp.13549 -
m commentaire
```

TRACIP
Technologies & Services d'Investigation

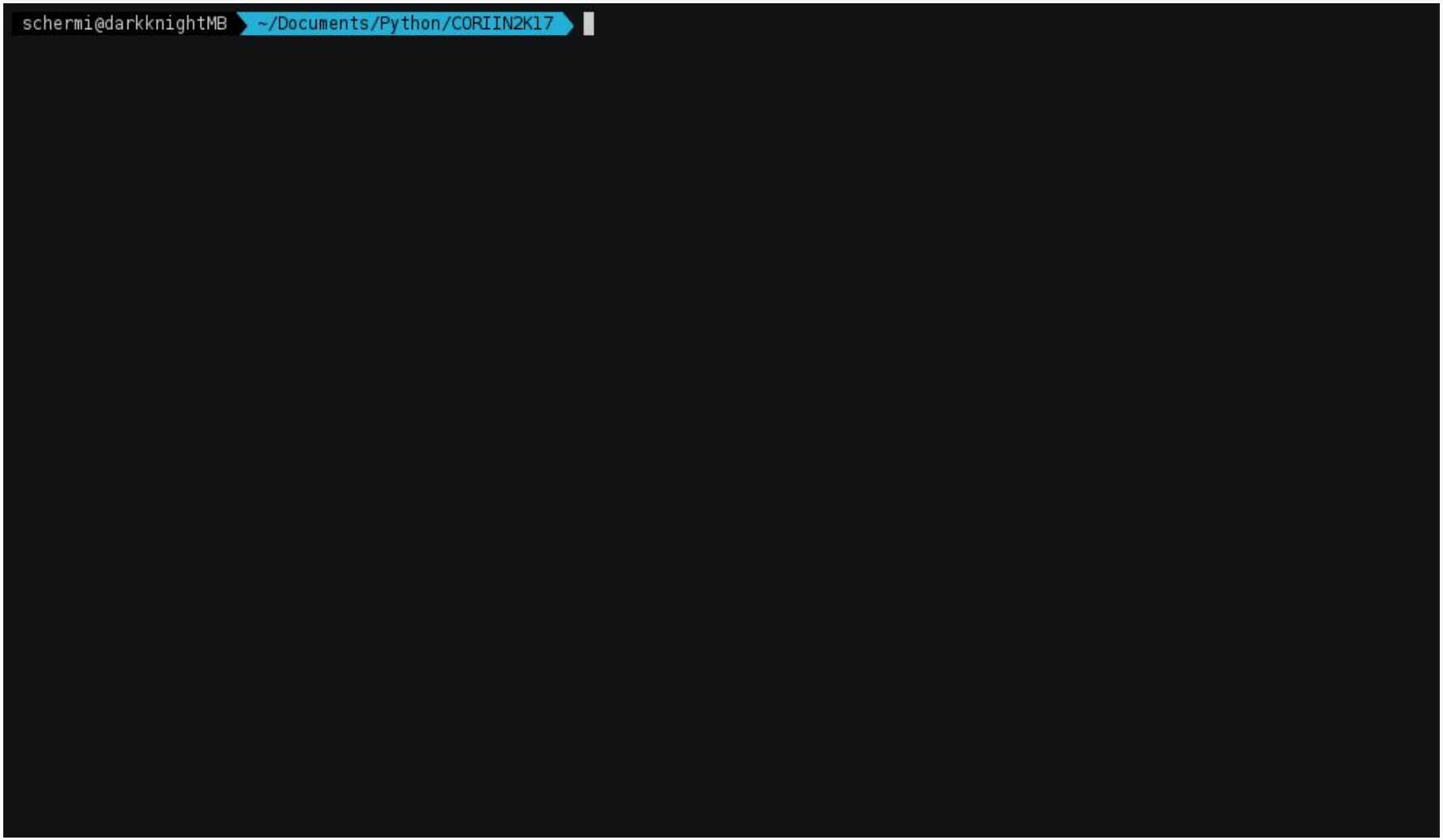
>_ Chat : Message

TRACIP
Technologies & Services d'Investigation

>_ Chat : Participants

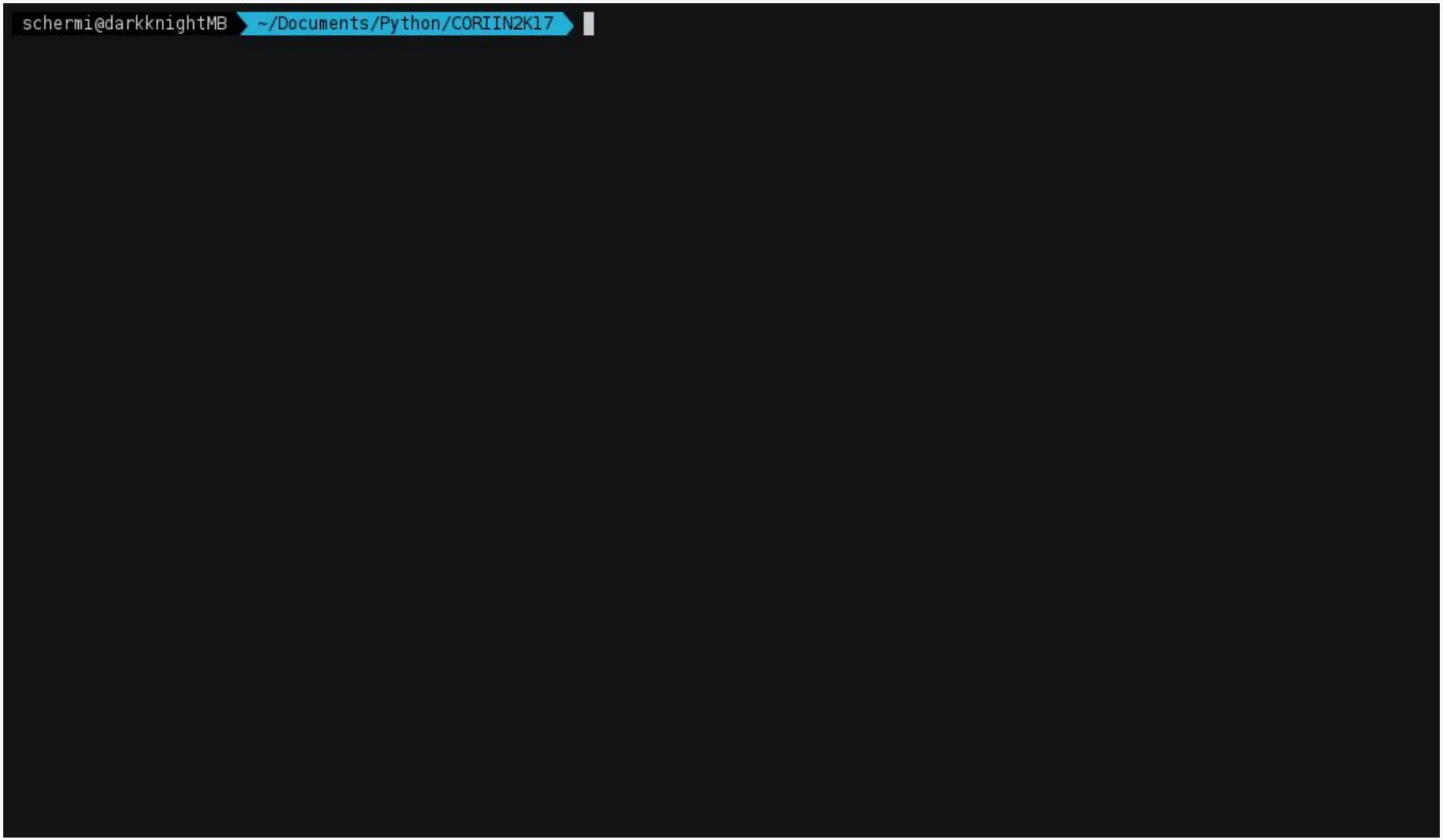
TRACIP
Technologies & Services d'Investigation

>_ Edition utilisateur



TRACIP
Technologies & Services d'Investigation

>_ Edition participant



TRACIP
Technologies & Services d'Investigation

>_ 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

TRACIP
Technologies & Services d'Investigation

>_ QUESTIONS ?

(BB)?

William Shakespeare