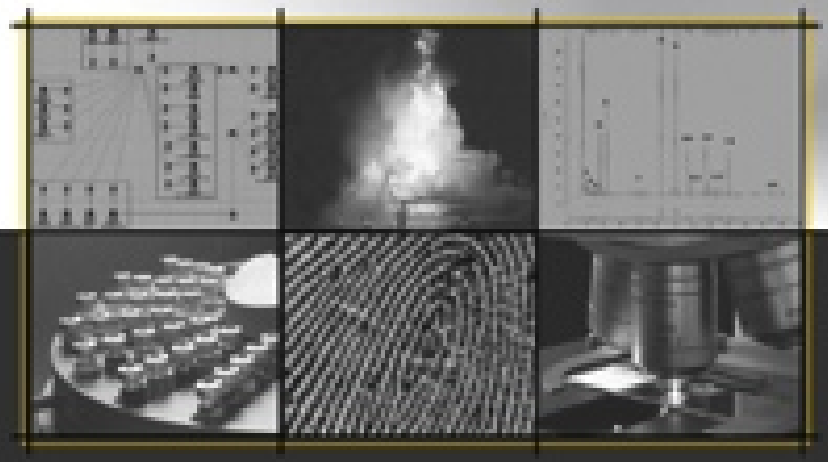
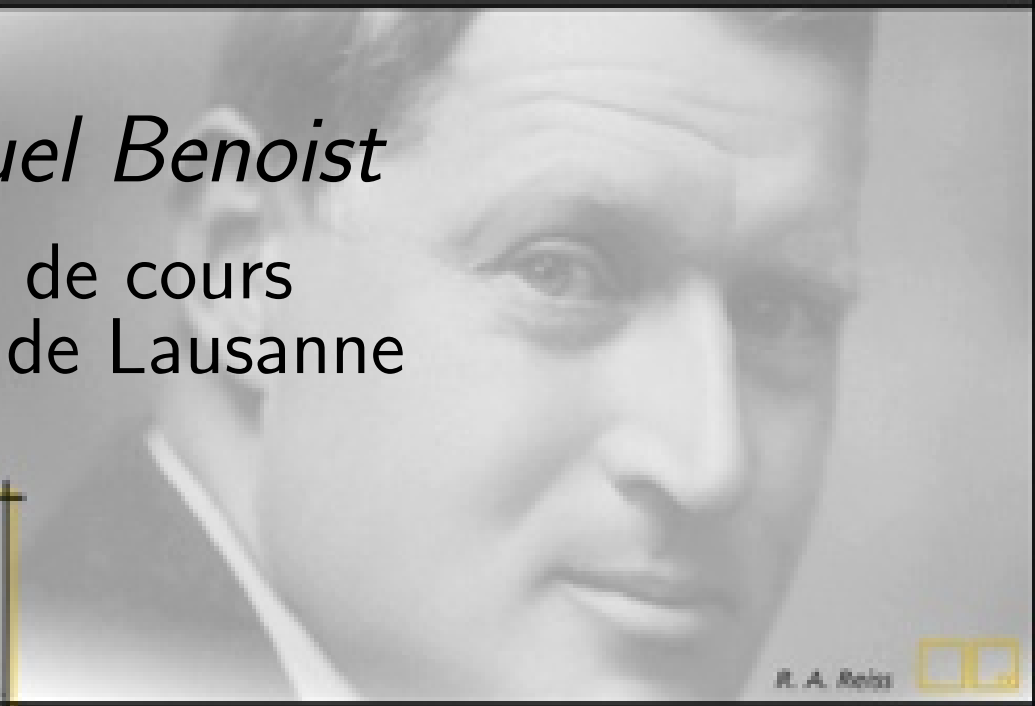
Traces sur le client

Emmanuel Benoist

Chargé de cours
Université de Lausanne

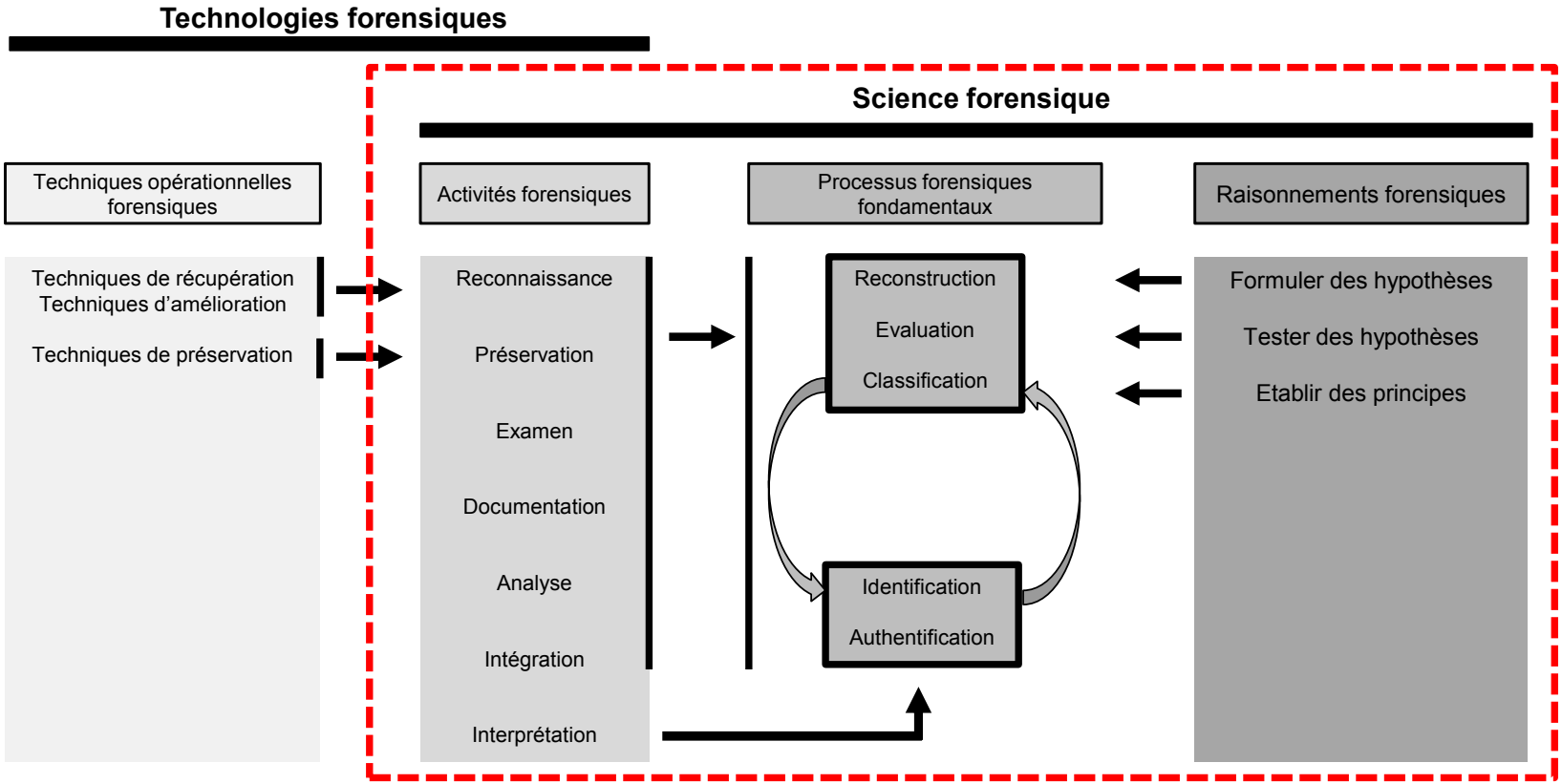




ESC école des sciences criminelles

UNIL | Université de Lausanne

Processus OSAC



Source : Slides partie David-Olivier Jaquet-Chiffelle

Outline

Traces sur le client

- **Lors d'une saisie, il faut prouver quel ordinateur a fait quoi?**
  - L'adresse IP seule n'est pas suffisante
  - Souvent beaucoup de systèmes sur un routeur
  - Parfois des malwares ouvrent des portes pour des externes (bot nets)
- **Beaucoup de traces restent sur un ordinateur**
  - Cookies
  - Pages en Cache
  - Historique
  - ...

Outline

Cookies

- **Petite information**
  - Envoyée par le serveur
  - Stockée par le client
  - Renvoyée à chaque requête
- **Exemples d'usage**
  - Identifiant de session
  - Identifiant d'utilisateur
  - Reconnaissance d'utilisateur (remember me)

Cookies

- **Informations contenues dans les cookies:**
  - le domaine du serveur;
  - le répertoire vers lequel le cookie doit être envoyé;
  - la durée de validité.
- **Stockés à une place différente pour chaque browser,**
  - toujours dans le répertoire de l'utilisateur,
  - spécifiques pour chaque utilisateur,
  - doivent rester entre deux sessions,
  - Écrits sur le disque dur.
- **Répertoire utilisateur (dans la suite : $\sim$)**
  - `/home/<username>/` sur Linux
  - `/Users/<username>/` sur Mac OS X
  - `C:\Documents\<username>\` Microsoft Windows 2000, XP and 2003
  - `C:\Users\<username>\` Windows Vista et 7

Lire les cookies I

- **Firefox**
  - Sur un Mac: `~/Library/Application Support/Firefox/Profiles/<profile folder>`
  - Sur Linux : `~/snap/firefox/common/.mozilla/firefox/<profile folder>`
- **FIle: cookies.sqllite**
  - Base de donnée SQLite
  - Une seule table : `moz_cookies`

Lire les cookies II

- **Visualiseur de fichier sqlite**
  - Installez `sqlitebrowser` (avec `apt install`)
  - Affiche les tables dans le fichier
  - Affiche pour chaque table, son contenu
  - Donne la possibilité d'executer des requêtes SQL
- **Regarder à l'intérieur du fichier sqlite**
  - `sqlitebrowser cookies.sqlite`

Cookies: Informations intéressantes

- **Description de la ressource**
  - `baseDomain`
  - `host`
  - `path`
- **Accès à la ressource**
  - `creationTime`
  - `lastAccessed`

Cookies dans Google Chrome

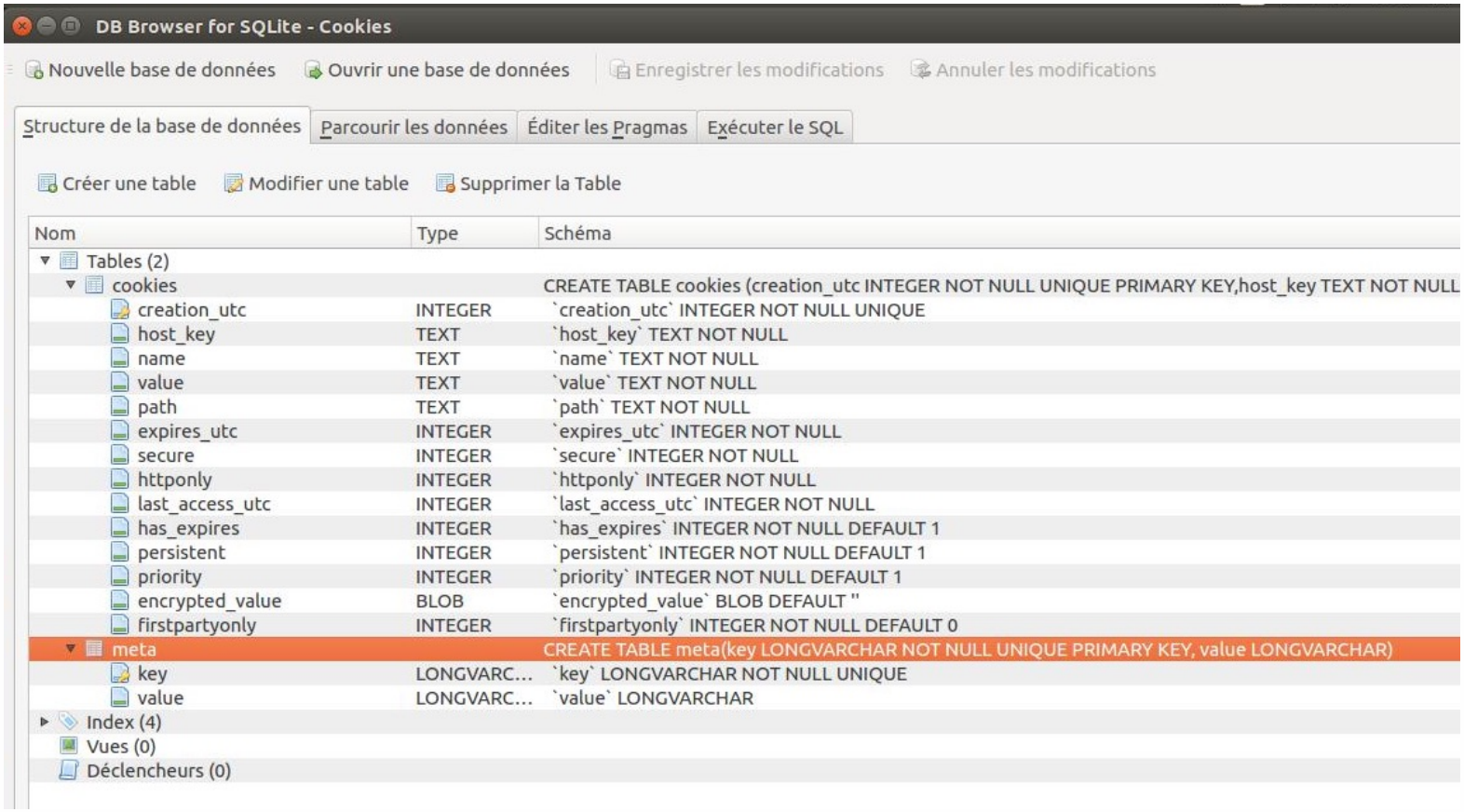
- **Chemin**
  - Sur Mac OS X:
    ~ /Library/Application Support/Google/Chrome/Default/Cookies
  - Sur Windows

    `C:\Users\<username>\AppData\Local\Google\Chrome\User Dat`
  - Sur Linux

    `~/.config/google-chrome/Default/Cookies`
- **Fichiers SQLite**

Cookies dans Google ChromeII

- **Structure de la table**



Nom	Type	Schéma
Tables (2)		
cookies		CREATE TABLE cookies (creation_utc INTEGER NOT NULL UNIQUE PRIMARY KEY,host_key TEXT NOT NULL
creation_utc	INTEGER	`creation_utc` INTEGER NOT NULL UNIQUE
host_key	TEXT	`host_key` TEXT NOT NULL
name	TEXT	`name` TEXT NOT NULL
value	TEXT	`value` TEXT NOT NULL
path	TEXT	`path` TEXT NOT NULL
expires_utc	INTEGER	`expires_utc` INTEGER NOT NULL
secure	INTEGER	`secure` INTEGER NOT NULL
httponly	INTEGER	`httponly` INTEGER NOT NULL
last_access_utc	INTEGER	`last_access_utc` INTEGER NOT NULL
has_expires	INTEGER	`has_expires` INTEGER NOT NULL DEFAULT 1
persistent	INTEGER	`persistent` INTEGER NOT NULL DEFAULT 1
priority	INTEGER	`priority` INTEGER NOT NULL DEFAULT 1
encrypted_value	BLOB	`encrypted_value` BLOB DEFAULT ''
firstpartyonly	INTEGER	`firstpartyonly` INTEGER NOT NULL DEFAULT 0
meta		CREATE TABLE meta(key LONGVARCHAR NOT NULL UNIQUE PRIMARY KEY, value LONGVARCHAR)
key	LONGVARC…	`key` LONGVARCHAR NOT NULL UNIQUE
value	LONGVARC…	`value` LONGVARCHAR
Index (4)		
Vues (0)		
Déclencheurs (0)		

Cookies avec Internet Explorer

- **Trouver les fichiers**

  `C:\Users\<username>\AppData\Roaming\Microsoft\Windows\C`

- **Les cookies sont stockés en clair**
  - Un fichier par cookie
  - Données en clair

Cookie, pour quoi faire?

- **Cookie = une requête**
  - Pour télécharger une page comme “20minutes.ch”, on reçoit 40 cookies du monde entier,
  - Correspondent à chaque requête
  - Pour des images (ou plus souvent un script JavaScript)
- **Cookie $\neq$ page visitée**
  - Cookie est placé automatiquement
  - il suffit d’une requête

Les Cookies sont très puissants

- **Cookies utilisés pour l'identification d'un utilisateur**
  - Le site envoie un identifiant de session (par ex. : `SESSION_ID=238778dfkxy98`).
  - Le navigateur renvoie cet identifiant à chaque requête.
  - Le navigateur sait que c'est le même utilisateur : "Session".
- **Si on arrive à accéder aux cookies d'un suspect**
  - On peut utiliser les cookies.
  - On récupère toutes les sessions qui étaient ouvertes.
  - On accède avec les droits de l'utilisateurs à ses comptes ouverts.
  - Google, Facebook, Instagram, Twitter, ...

Outline

- Introduction
- Les Cookies
- Historique et cache
- Autres traces
- Possibilité de cacher ces informations
- Conclusion

Historique de navigation

- **Tous les browser gardent cette information**
  - Pour faire de l'autocompletion
  - Pour faire des aides contextuelles
  - Pour pouvoir faire des *"Back"*s
- **Firefox stocke dans le fichier** `places.sqlite`
- **Chrome dans le fichier** `History`

Cache des pages

- **Les pages (et autres ressources) sont gardées en mémoire quelques temps**
  - But optimiser la visite d'un site
  - On stocke le résultat de la requête
  - Fait gagner du temps plus tard
- **Utiles pour l'optimisation des sites**
  - Pages gardées pour faire des *"Back"*s
  - Images ou CSS réutilisées pour d'autres pages
- **Optimisation**
  - Lorsque une page est chargée
  - Elle demande des ressources (images, styles, JavaScripts, ...)
- **Si la ressource est dans le cache:**
  - on peut soit l'y prendre (et ne pas envoyer de requête au serveur),
  - soit demander au serveur si la version est toujours valide

Usage du cache

- **Informations sur une ressource dans le cache**
  - URL de la ressource
  - Date de production
  - Date de validité (si fournie par le site)
  - Numéro de version (= ETag)
- **Si le client a besoin d'une ressource**
  - Regarde si elle est dans le cache
  - Si elle est encore valide: utiliser le cache
  - Sinon, demander au serveur la ressource en indiquant la version de celle en cache
  - Si le serveur a une version plus neuve, il renvoie une nouvelle
  - Sinon, utiliser la version en cache.

Outline

Mots de passes

- **Stockés automatiquement par les browsers**
  - Account stocké pour de nombreux sites
  - Indique aussi: ne jamais stocker
- **Indication très forte**
  - L'utilisateur a visité une page
  - Accès à son login et password
  - Ou a explicitement refusé le stockage
- **Indique une action sur le site**
  - Si une entrée existe: L'utilisateur s'est logué sur le site
  - Même si l'entrée est `ne pas sauvegarder` c'est une information

Stockage de données HTML5

- **Nouvelles fonctionnalités**
  - Possibilité de stocker des informations sur le client
  - Accessible uniquement au JavaScript qui vient de ce serveur
- **Forme**
  - ensemble de paires variable=valeur
  - Base de donnée SQL
- **Usage**
  - En JavaScript, on accède à des données
  - Depuis le serveur (Ajax) / Depuis l'utilisateur (ce qu'il tape)
  - Ces données sont stockées sur le client
  - JavaScript peut toujours lire ces informations
  - Ces données ne sont pas renvoyées à chaque fois ($\neq$ cookies)

Outline

- Introduction
- Les Cookies
- Historique et cache
- Autres traces
- Possibilité de cacher ces informations
- Conclusion

Peut-on cacher ces infos?

- **Configuration Tor**
  - Navigateur configuré pour Tor
  - Minimum d'information stockée
- **Config Parano:**
  - Pas d'historique
  - Pas de cookie
  - Pas de cache
  - Pas de password
  - Pas possible avec tous les navigateurs.

Outline

- Introduction
- Les Cookies
- Historique et cache
- Autres traces
- Possibilité de cacher ces informations
- Conclusion

Conclusion

- **De nombreuses traces sont laissées en surfant**
  - Cache, historique, cookies, ...
- **Certaines traces sont cachées**
  - Entrée DNS, Certificat, mot de passe stocké (ou pas)
- **Information obtenue**
  - Une abscence de trace ne signifie pas que rien ne s'est passé
  - Si des traces cohérentes sont découvertes
  - Alors, seul un service très puissant est capable de les définir.

Bibliographie

- Site de Firefox
- Site Mircosoft (documentation IE)
- Site google Chrome