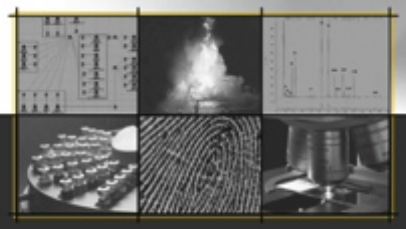
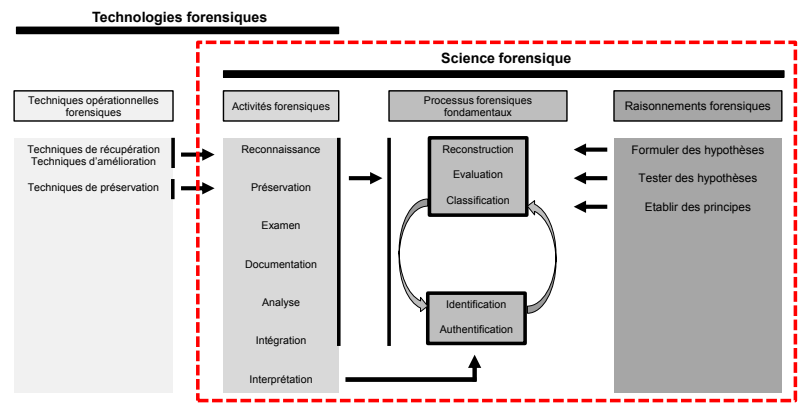
Internet: un reseau, des traces.

Emmanuel Benoist

Chargé de cours
Université de Lausanne



Processus OSAC



Source : Slides partie David-Olivier Jaquet-Chiffelle

Outline

Introduction

- **Qu'est-ce qu'Internet?**
  - "Internet, mais c'est le Web! " ?
- **Plus sérieusement**
  - Un réseau de réseaux inter-connectés
  - Créé par les militaires américains pour avoir un réseau sans "single point of failure"
  - Une pile de protocoles
  - Un ensemble de services offerts aux ordinateurs en réseaux
- **Exemples de services sur Internet**
  - Le Web, le mail, l'échange de fichiers,
  - la voiceOverIP
  - les applications sur smartphones,
  - ...

Motivation

- **Sur le web, tout le monde est anonyme**
  - Du moins le croit on !
- **Quantité de données publiques sont déjà accessibles sur tout le monde**
  - LinkedIn, Instagram, Facebook, Moneyhouse (registre du commerce)
  - En dehors du domaine de notre cours.

Internet une mine de traces

- **Sniffing**
  - Écouter en direct les communications
- **Traces sur l'ordinateur**
  - Fichier téléchargés
  - Mails
  - Fichiers cache
  - Cookies
  - Historique des pages visitées (et des recherches)
- **Traces sur le réseau**
  - Server logs
  - Firewall logs
  - DNS logs

Limitations (dernier cours)

- **Possibilité d'effacer/falsifier certaines traces sur l'ordinateur**
  - Effaçage du cache automatique
  - Effaçage des cookies à la fin de la session
- **Possibilité d'agir anonymement sur internet**
  - Proxy server
  - Tor
  - VPN
  - ...

Outline

Le protocole Internet (IP)

- **Détails vus l'année dernière**
  - Cours de première annéej. *"Bases des réseaux"*
  - Internet = Des hôtes reliés par des lignes de communication, entre lesquels des paquets sont envoyés.
- **Comprend 5 couches**
  - Chaque couche contient plusieurs protocoles différents
  - Les protocoles sont basés sur les couches inférieures

IP (couche inférieure)

- **Couche physique**
  - transmission des signaux physiques
  - Signal électromagnétique (avec cable ou sans cable), signal lumineux, ...
- **Exemples:**
  - Twisted pair avec connecteurs RJ45
  - Cable coaxial
  - Wifi
  - Signaux lumineux sur fibre optique

IP (couches intermédiaires)

- **Couche Data Link**
  - Responsable de la communication directe entre deux points
  - utilise l'adresse MAC de chaque machine
  - Cette adresse est donnée à la fabrication de chaque machine
  - Elle n'est généralement pas changée durant la vie d'une machine
  - exemple: 60:c4:37:7a:eb:be
- **Internet Layer**
  - équivalente à la couche réseau
  - Chaque ordinateur reçoit une adresse unique: adresse IP
  - 147.87.127.1 par exemple (IP V4)
  - ou 2001:620:500::20 (IP V6)
  - Les adresse IP V4 étant rare, les ISP donnent souvent des adresses dynamiques (à chaque fois que le client se reconnecte)
  - responsable du routage dans le net

IP (couches supérieures)

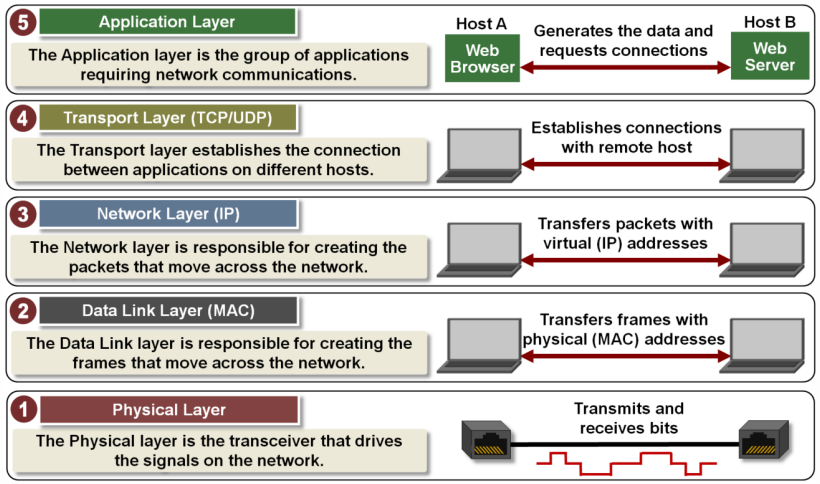
- **Couche transport**
  - 2 implémentations: UDP et TCP
  - **UDP** Universal Datagram Protocol
  - But: envoyer le plus de données le plus vite possible
  - Moyen: envoyer les données sans attendre de confirmation de l'arrivée
  - Usage: Broadcasting (internet radio ou TV)
  - **TCP** Transmission Control Protocol
  - Vérification de l'arrivée des paquets
  - Les paquets perdus sont renvoyés
- **Couche application**
  - Combine les couches applications et présentation
  - Exemples: HTTP, POP-3, IMAP, SMTP, FTP

Couches Protocole IP (I)

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc...	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

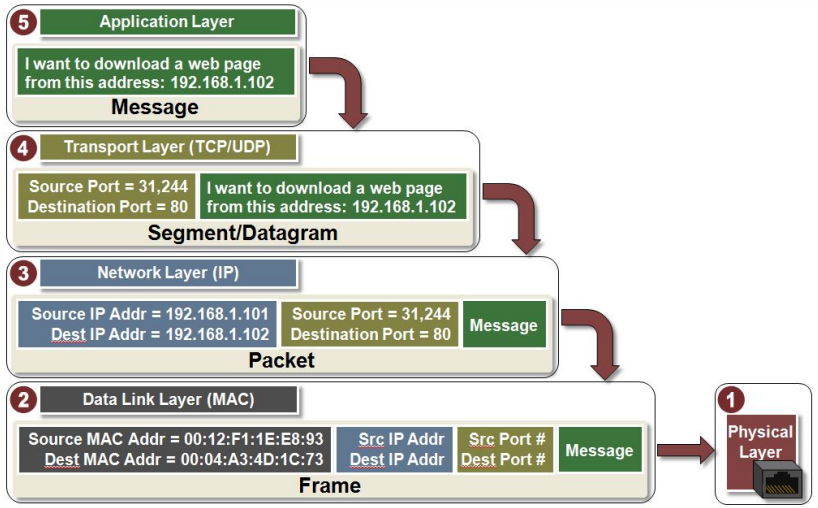
Source : https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

Couches Protocole IP (II)



Source : https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

Couches Protocole IP (III)



Source : https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

Accéder à un site: Connexion

- **Le client ouvre un "socket" TCP/IP avec le server**
  - Le client connecte le port 80 de la machine `147.87.250.142`
  - Il communique en HTTP sur ce port pour demander à récupérer une page (i.e. requête GET)

Les ports

- **Un port = un poste téléphonique interne dans une entreprise**
  - À chaque port correspond un service
  - Les ports < 1024 sont réservés
- **Exemples de ports standards**
  - Web port 80 (http) et port 443 (https)
  - FTP port 21 (transfert de fichiers)
  - SSH port 22 (shell sécurisé à distance)
  - SMTP port 25 (envoi de mail)
  - DNS port 53 (annuaire général des noms de domaines)

Exemples de protocoles

- **e-mail**
  - SMTP : envoi de courrier
  - IMAP : réception de courrier (reste sur le serveur)
  - POP-3 : réception de courrier (transféré sur le client)
- **Connexion à distance**
  - Telnet / SSH
- **Transfert de fichier**
  - FTP / SFTP
- **Web**
  - HTTP / HTTPS

Outline

Domain Name Service - DNS

- **Gigantesque annuaire**
  - Impossible de connaître les adresses IP de tous les serveurs
  - idée: donner un nom unique à chaque machine
- **Organisation hiérarchique**
  - 13 serveurs de top niveau
  - Des serveurs pour les top level domains (TLD) : `.ch`, `.com`, `.net`, `.org`
  - Qui pointent sur les serveurs de nom de domaine: `unil.ch`, `benoist.ch`, `vip.ch`.

Accéder à un site: DNS

- **Résolution de nom de domaine**
  - Exemple: accéder au serveur `www.ti.bfh.ch`
  - Notre client contacte son DNS-Serveur
- **Actions entreprises par le serveur DNS local**
  - Accéder au serveur de top niveau
  - demander l'adresse du serveur de noms `.ch`
  - Contacter le serveur de Switch (`.ch`)
  - demander l'adresse du serveur de noms `.bfh.ch`
  - Contacter le serveur de la BFH (`.bfh.ch`)
  - demander l'adresse du serveur de noms `.ti.bfh.ch`
  - Contacter le serveur de nom du sous-domaine `.ti.bfh.ch`
  - demander l'adresse de la machine `www.ti.bfh.ch`
- **Retour du serveur au client**
  - L'adresse IP du serveur est: `147.87.250.142`

(Pour plus de détails, c.f. cours de première année)

DNS I

- **Le DNS est appelé automatiquement par le client**
  - Chaque fois qu'il a besoin
  - L'adresse est demandée au serveur DNS local
- **Possiblité de voir l'adresse**
  - Faire un ping

```
[bie1@MacBook-Pro-de-Emmanuel courant]$ ping www.unil.ch
PING www.unil.ch (130.223.27.47): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
```

  - Ping est refusé par le serveur de l'UniL (raison de sécurité)
  - Mais l'adresse apparait en clair à l'écran

DNS: Exemple

- **DNS de benoist.ch**
  `http://testdns.fr/?ndd=benoist.ch`

Outline

Nslookup I

- **Permet de connaitre le nom d'une machine**
  - On donne une adresse IP
  - Donne le nom de la machine
- **Exemple**

```
$ nslookup 194.150.248.53
Server:  89.2.0.1
Address: 89.2.0.1#53

Non-authoritative answer:
53.248.150.194.in-addr.arpa name = srv1.tophost.ch.

Authoritative answers can be found from:
```


Nslookup II

- **Une machine a plusieurs noms**
  - Plusieurs DNS peuvent pointer sur la même adresse IP
  - Serveur multi-domaine par exemple
- **Nslookup donne un des noms en retour**
  - Souvent le nom dans le domaine du hoster.
  - Donc donne le nom du hoster.

Nslookup: Exemple

```
$ ping www.vip.ch
PING www.vip.ch (83.166.138.104): 56 data bytes
64 bytes from 83.166.138.104: icmp_seq=0 ttl=52 time=23.16
.....

$ nslookup 83.166.138.104
Server:  89.2.0.1
Address: 89.2.0.1#53

Non-authoritative answer:
104.138.166.83.in-addr.arpa name = h2web121.infomaniak.ch.

Authoritative answers can be found from:
```


Whois?

- **Les serveurs DNS gardent les informations suivantes**
  - Nom de domaine
  - Adresse IP des serveurs DNS du domaine
- **Mais les "registrars" ont aussi les informations suivantes (pour la facturation/gestion)**
  - Propriétaire du site
  - Adresse
  - Contact technique pour le site
  - Adresse
- **Le protocole "Whois"**
  - Couplé avec le protocole DNS
  - Permet de connaître les informations sur un site web

La commande whois

- whois retourne le serveur responsable pour les données d'un site

```
$ whois ricardo.ch
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
refer:        whois.nic.ch
domain:       CH
organisation: SWITCH The Swiss Education & Research Networl
....
whois:        whois.nic.ch
status:       ACTIVE
...
# whois.nic.ch
Requests of this client are not permitted. Please use https
```


Quelques serveurs "whois"

- **Switch (pour tous les sites en Suisse)**
  - `whois.nic.ch`
- **Internic (sites généraux)**
  - `http://www.internic.net/whois.html`
  - indique l'adresse du registrar
- **Example: google.com**
  - Registrar : Markmonitor
  - Whois server: `https://www.markmonitor.com/`

Limitations du Whois

Protection de la sphère privée

```
 [bie1@MacBook-Pro courant]$ whois lamagiepourlesenfants.c
....
Domain Name: lamagiepourlesenfants.com
Registry Domain ID: 1617524054_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.psi-usa.info
Registrar URL: https://www.psi-usa.info
....
Domain Status: clientTransferProhibited https://www.icann.
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: FR
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
```


Géolocalisation IP

- **Les ranges d'adresses sont réservés par des ISP**
  - Adresses de classes A, B, C, ou D
  - redistribuées en sous-réseaux
- **Des bases de données rassemblent ces informations**
  - Elles sont rassemblées dans le monde entier
  - Elles sont corrélées avec des données de géolocalisation

Géolocalisation IP (Cont.)

- **Possibilité de géolocaliser une adresse IP**
  - De nombreux services disponibles
  - par example : `http://www.localiser-ip.com/` ou `http://www.ip-adress.com/`, ...
- **Localisons le site de l'UniL**
  - Resolvons le nom `www.unil.ch`

```
[bie1@MacBook-Emmanuel courant]$ ping www.unil.ch
PING www.unil.ch (130.223.27.47): 56 data bytes
Request timeout for icmp_seq 0
```

  - Accédons aux informations:
    `http://www.localiser-ip.com/?ip=130.223.27.47`
    `http://www.ip-adress.com/ip_tracer/130.223.27.47`

Outline

Conclusion

- **Internet Protocole**
  - Plusieurs types d'identités
  - Nom de machine (dont nom de domaine)
  - adresse IP
  - adresse MAC
- **Informations sur les serveurs**
  - Qui est le responsable
  - Comment le hosting est fait
- **Attention**
  - De nombreuses informations peuvent être fausses
  - Les registrars ne vérifient aucune des informations
  - Selon le niveau de Certificat, aucune information sur l'identité de l'opérateur du site peut n'avoir été vérifiée.

Traces

- **Traces sur le réseau**
  - Log files sur le serveur
  - Trafic sur le réseau
- **Traces sur le PC (ou la tablette/ téléphone/etc.)**
  - Historique
  - Pages de cache
  - cookies
  - DNS entries
  - certificats
  - Bases de données locales

Bibliographie

- **ISO/OSI et Internet Protocole**
  - **Digital Forensics**, Angus Marshall
- **TCP/IP Five-Layer Software Model Overview**
  `https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model`