Internet, Principes et Protocoles (IPP)

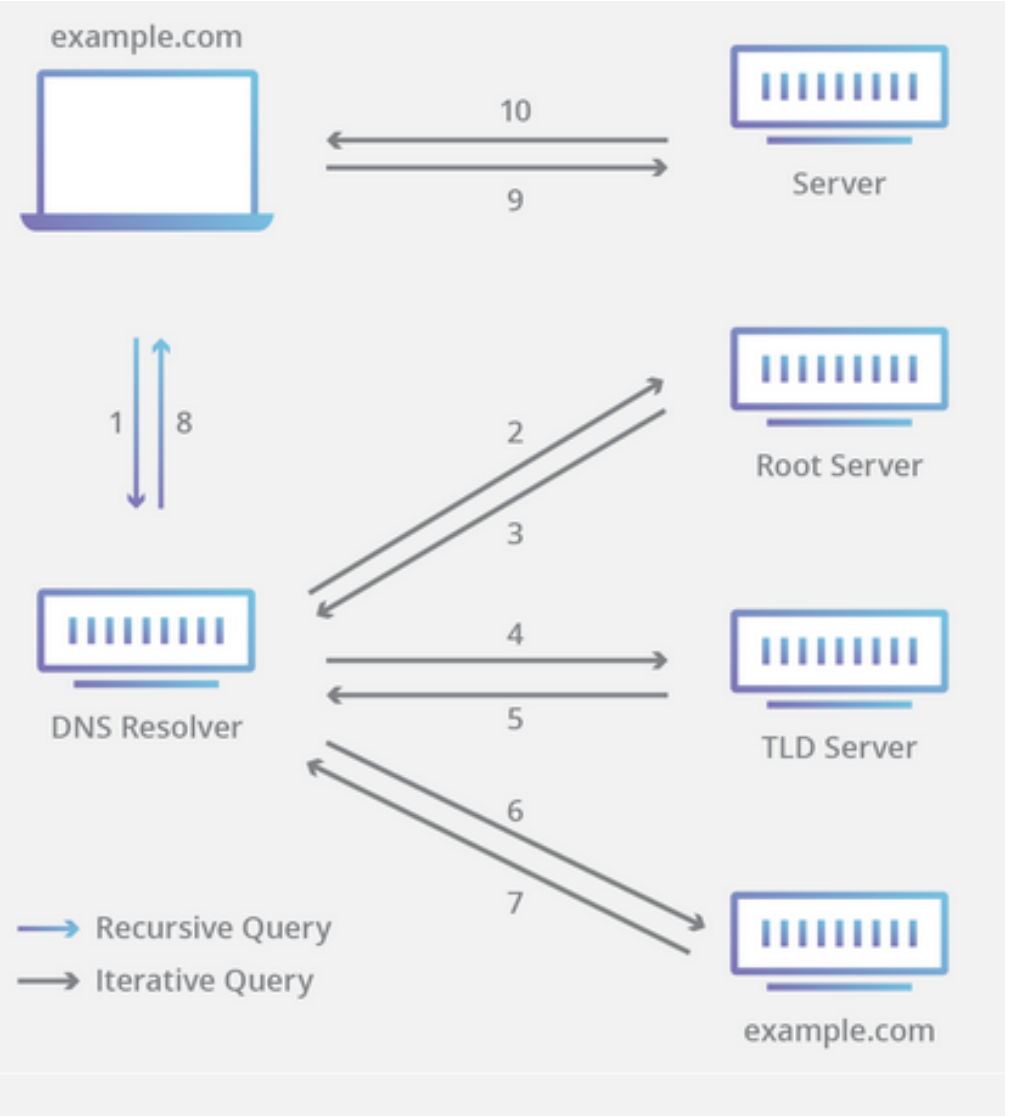
Application Layer

- Highest layer, allowing hosts to exchange different kind of information (sending emails, ssh, serving websites, REST APIs,...)
- Relying on the lower protocols for the transmit ion and management of the information.
- Often using on the client-server model

DNS In Practice

The 8 steps in an iterative DNS lookup:

- A user types ‘example.com’ into a web browser which sends the query to a DNS recursive resolver.
- The resolver then queries a DNS root nameserver.
- The root server then responds to the resolver with the address of a TLD DNS server (such as .com or .net), which stores the information for its domains.
- The resolver then makes a request to the .com TLD.
- The TLD server then responds with the IP address of the domain’s nameserver, example.com.
- The recursive resolver sends a query to the domain’s nameserver.
- The domain nameserver answers with the IP address for example.com
- The DNS resolver then responds to the web browser with the IP address



World Wide Web - URL

Uniform Resource Locator (URL)

generic syntax : <protocol>://<document>

protocol used to retrieve document from server

http is the most common one but others are frequently used

document indicates the server and the location of the document

<user>:<password>@<server>:<port>/<path>

<user> : optional username

<password> : optional password

<machine> : hostname or IP address of the server that hosts the document

<port> : optional port number

<path> : document location on server

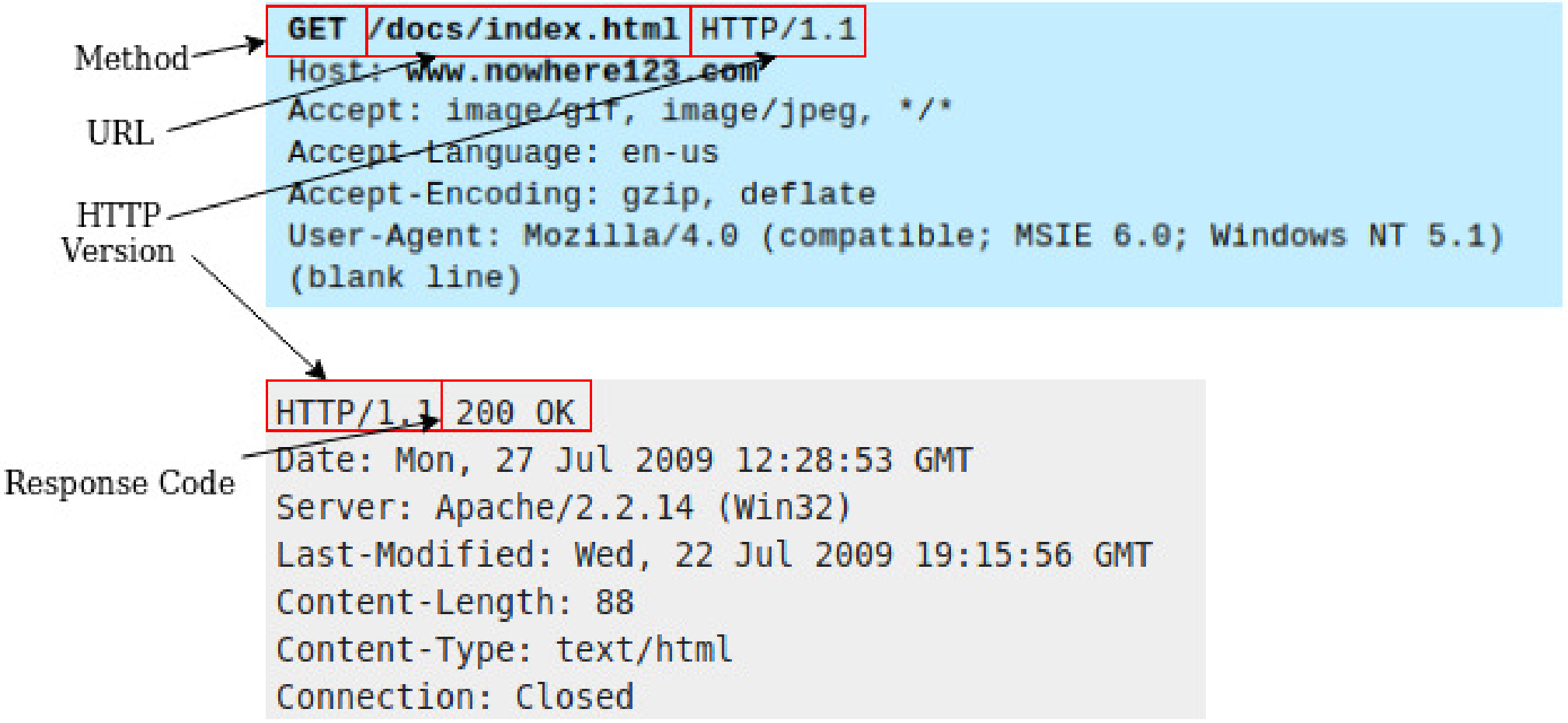
examples

http://www.info.ucl.ac.be

http://alice:secret@inl.info.ucl.ac.be:80/index.html

HTTP

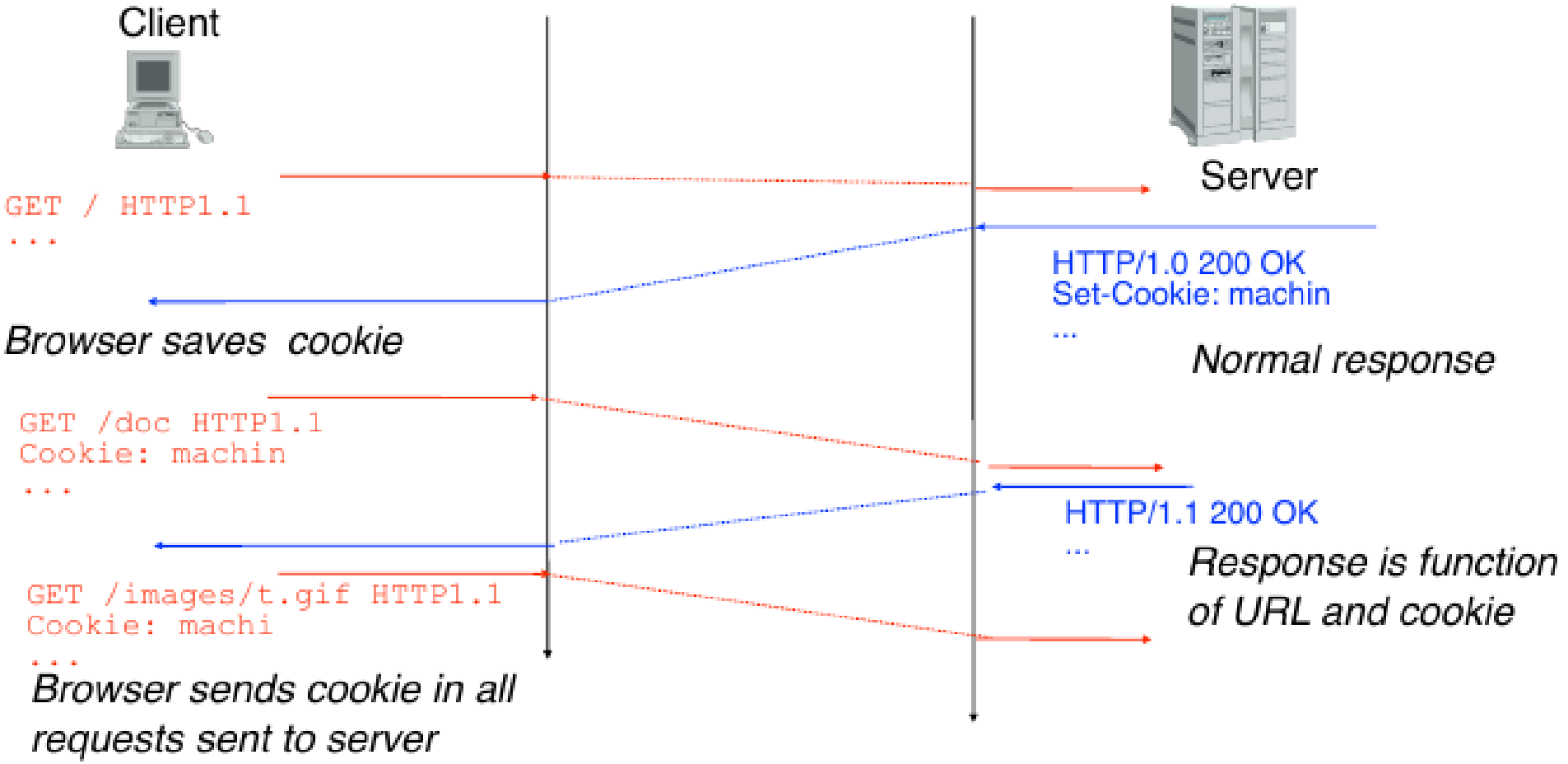
HTTP request and response example



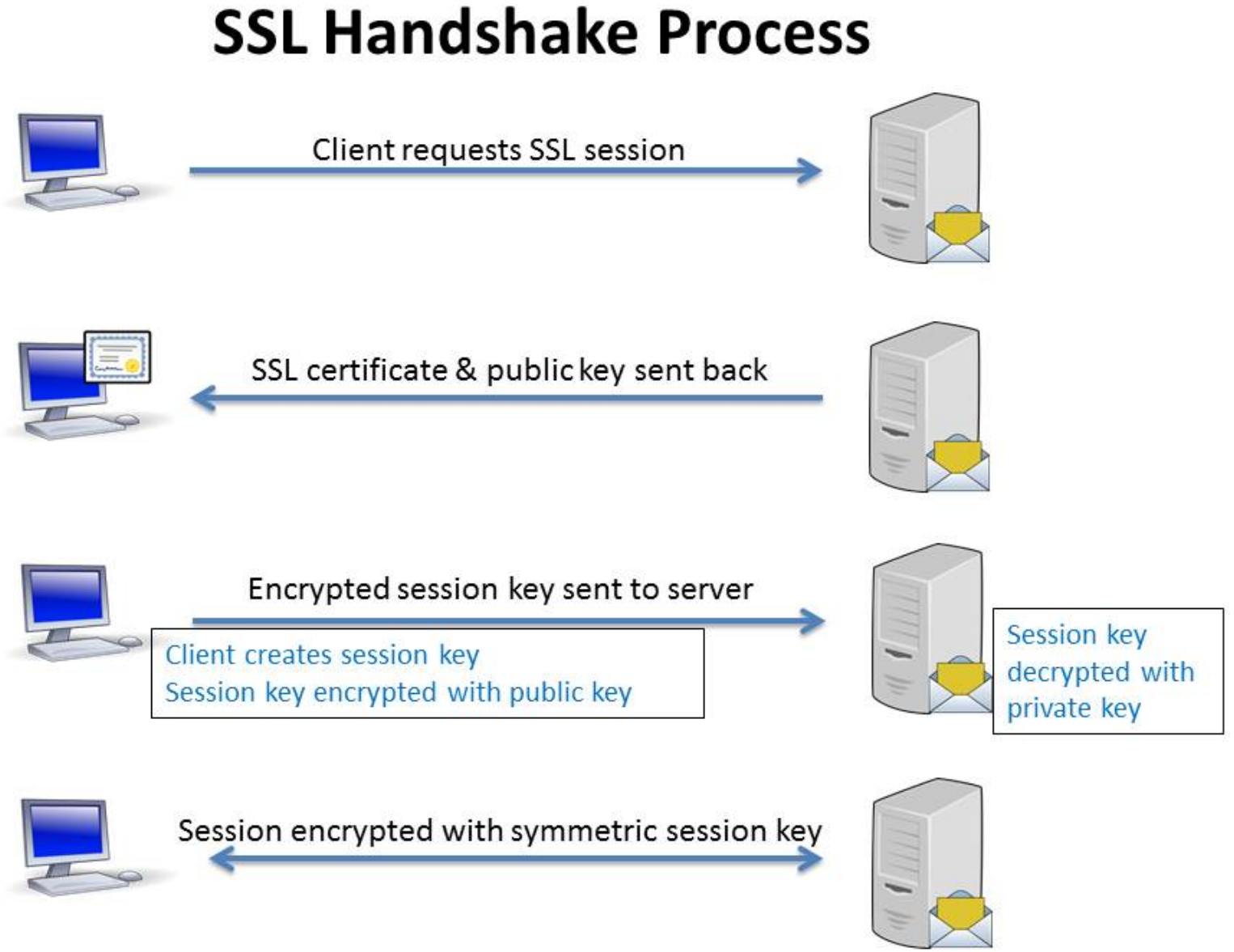
HTTP Methods

- GET: A client can use the GET request to get a web resource from the server.
- HEAD: A client can use the HEAD request to get the header that a GET request would have obtained.
- POST: Used to post data up to the web server.
- PUT: Ask the server to store the data.
- DELETE: Ask the server to delete the data.
- TRACE: Ask the server to return a diagnostic trace of the actions it takes.
- OPTIONS: Ask the server to return the list of request methods it supports.
- ...

Cookies


Client
Server
GET / HTTP1.1
...
HTTP/1.0 200 OK
Set-Cookie: machin
...
Browser saves cookie
Normal response
GET /doc HTTP1.1
Cookie: machin
...
HTTP/1.1 200 OK
...
Response is function of URL and cookie
GET /images/t.gif HTTP1.1
Cookie: machi
...
Browser sends cookie in all requests sent to server

TLS


SSL Handshake Process
Client requests SSL session
SSL certificate & public key sent back
Encrypted session key sent to server
Client creates session key
Session key encrypted with public key
Session key decrypted with private key
Session encrypted with symmetric session key

Question

- What happens when you type https://vinci.be/index.html in your browser? (uniquement la couche application)

Various Protocols

- NTP – Network Time Protocol: Designed to sync the clocks of computers.

- Telnet – Bi-directional text-based communication protocol. No authentication, unsecured. Usage: *telnet url port.*

  towel.blinkenlights.nl (port 80 and 666)

FTP – File Transfer Protocol

- Used to.. transfer files
- Can use SSL/TLS, beconing SFTP (secure FTP)
- Login using system users, or anonymous user (if enabled)
- Runs over TCP
- Default ports: 20 for data transfer and 21 for command port

FTP Commands

- HELP - help
- USER – to log in
- PASS – to log in
- LIST – list files
- CD – change directory
- GET – get file
- PUT – upload file
- QUIT – Bye bye

Secure Shell - SSH

- Telnet, but secure
- Uses public-private key for security
- Default port: 22
- An SSH client usually connects to a server running the SSH service. Usage: *ssh user@[url|IP]*
- On Windows, you can use PUTTY. All Unix systems support SSH by default
- Used to do remote system administration

Secure Copy - SCP

- Used to securely copy files over the network.
- Based on SSH
- Usage:

  scp SourceFile user@host:directory/TargetFile

  scp user@host:directory/SourceFile TargetFile
- GUI: Filezilla - example

Example SSH - SCP

- Connection to server
- Execute commands
- Check out apache log files
- SCP them

- SCP vs FTP
  - SSH Example

Remote Desktop Protocol

- RDP allows remote login with GUI
- Microsoft protocol
- Port 3389 – UDP and TCP
- Shodan example

Recap

- Telnet
- SSH – SCP
- NTP
- RDP
- FTP
- WHOIS - Example