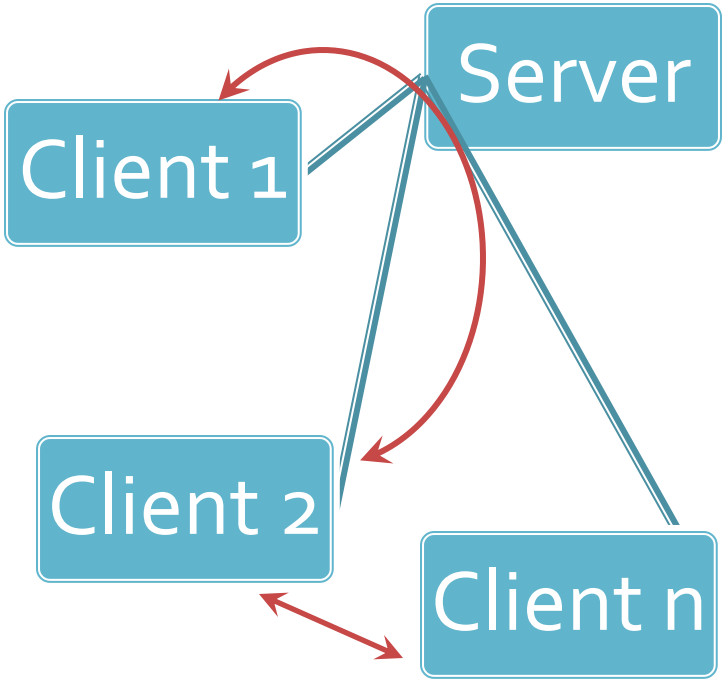
Curs 4

Tehnologii Web

Instant Messaging, Chat, Talk

- metoda **sincrona** de comunicare
- unele necesita un server care sa intermedieze comunicatiile
  - client – server – client
  - client – client
- IM – 1/1, paragraf
  - Yahoo
  - Microsoft
  - AOL
- Chat – 1/x, paragraf
- Talk – 1/1, caracter

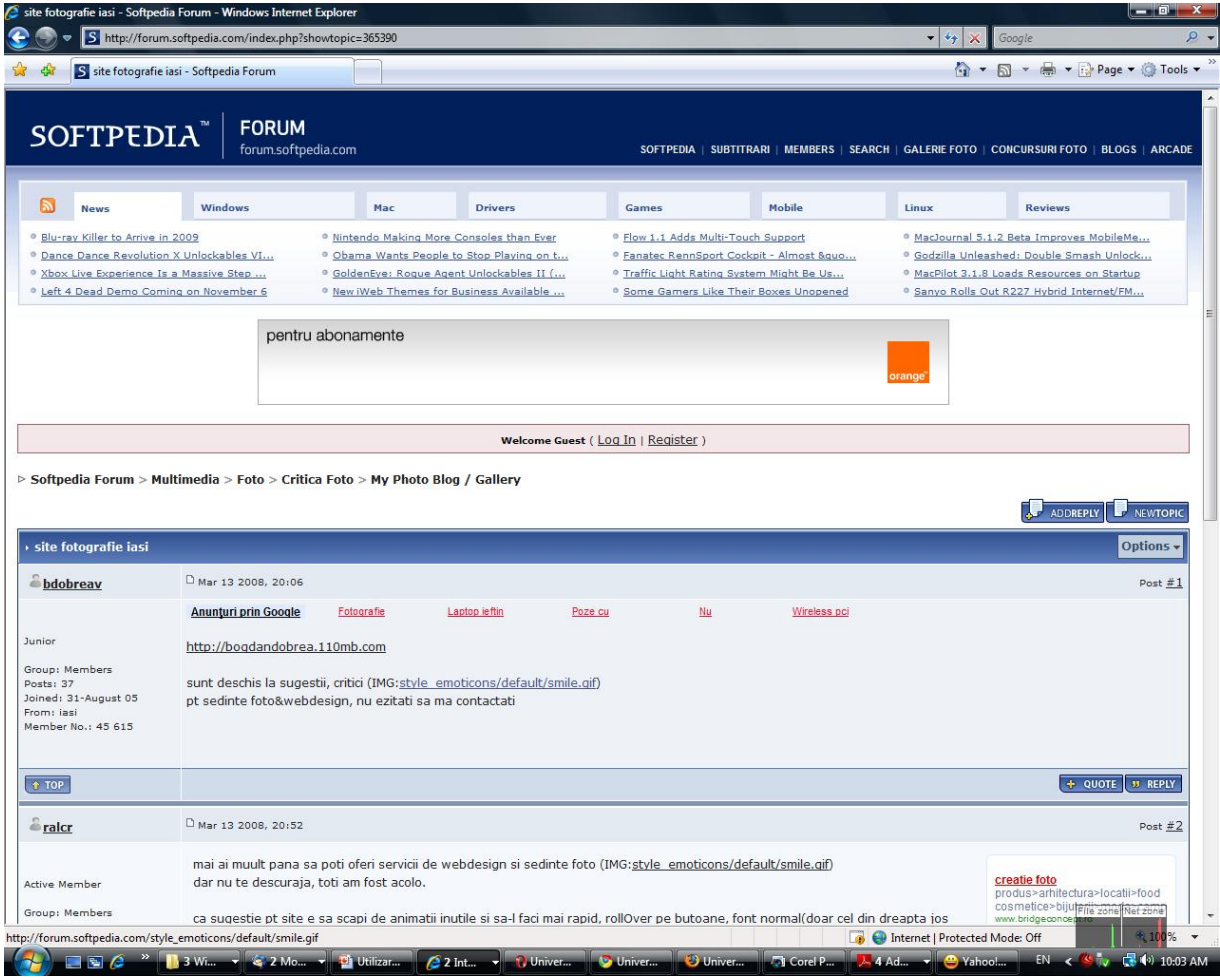


YM

- Yahoo Messenger
- http://messenger.yahoo.com
- emoticons
  - ☺ = :), ☹ = :(, ;-)
  - hidden emoticons: @};- , [-O< , ^:)^
- abrevieri
  - AFAIK – as far as I know
  - BRB – be right back
  - IIRC – if I recall correctly
  - IMHO – in my humble opinion
  - LOL – laughing out loud
  - ROTFL – rolling on the floor laughing
  - etc……

Forum

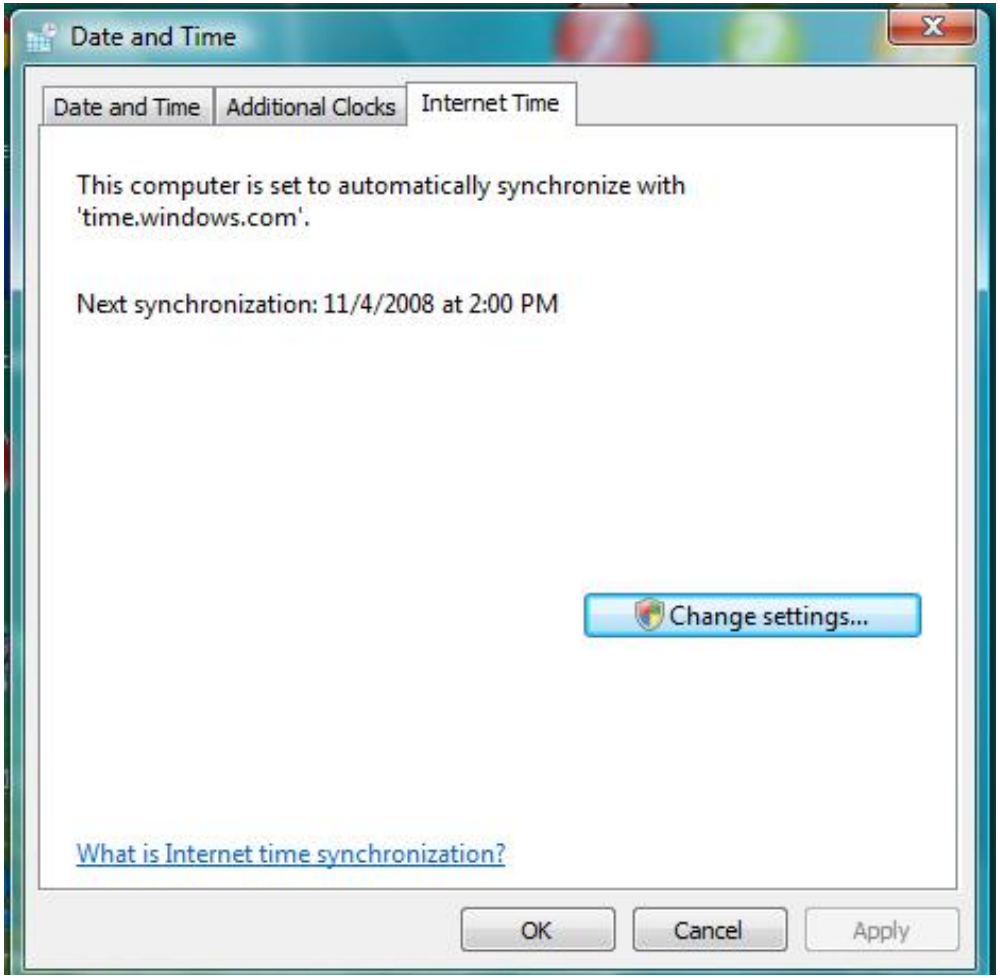
- Chat **asincron**
- Orientate pe domeniu
- Structura arborescenta (graf)
- Reguli (moderatori)
- Punct de intalnire pentru cei cu interese comune



FTP

- FTP – File Transfer Protocol
- Metoda **eficienta** de transmitere a datelor binare (MIME – 66%)
- Aplicatie client – server
  - fisierele sunt incarcate pe un server care le stocheaza
  - Cont: username:password@server
  - anonymous:adresa_de_email
  - **ftp://numecont:parola_in_clar@ftp.tuiasi.ro**
  - port tipic: 21
- Securitate
  - SSH – Secure Shell
  - SFTP – SSH file transfer protocol
  - SCP – Secure Copy Protocol
  - port tipic: 22
- Aplicatii
  - Browser-e
  - WinScp
  - Total Commander

Internet Time

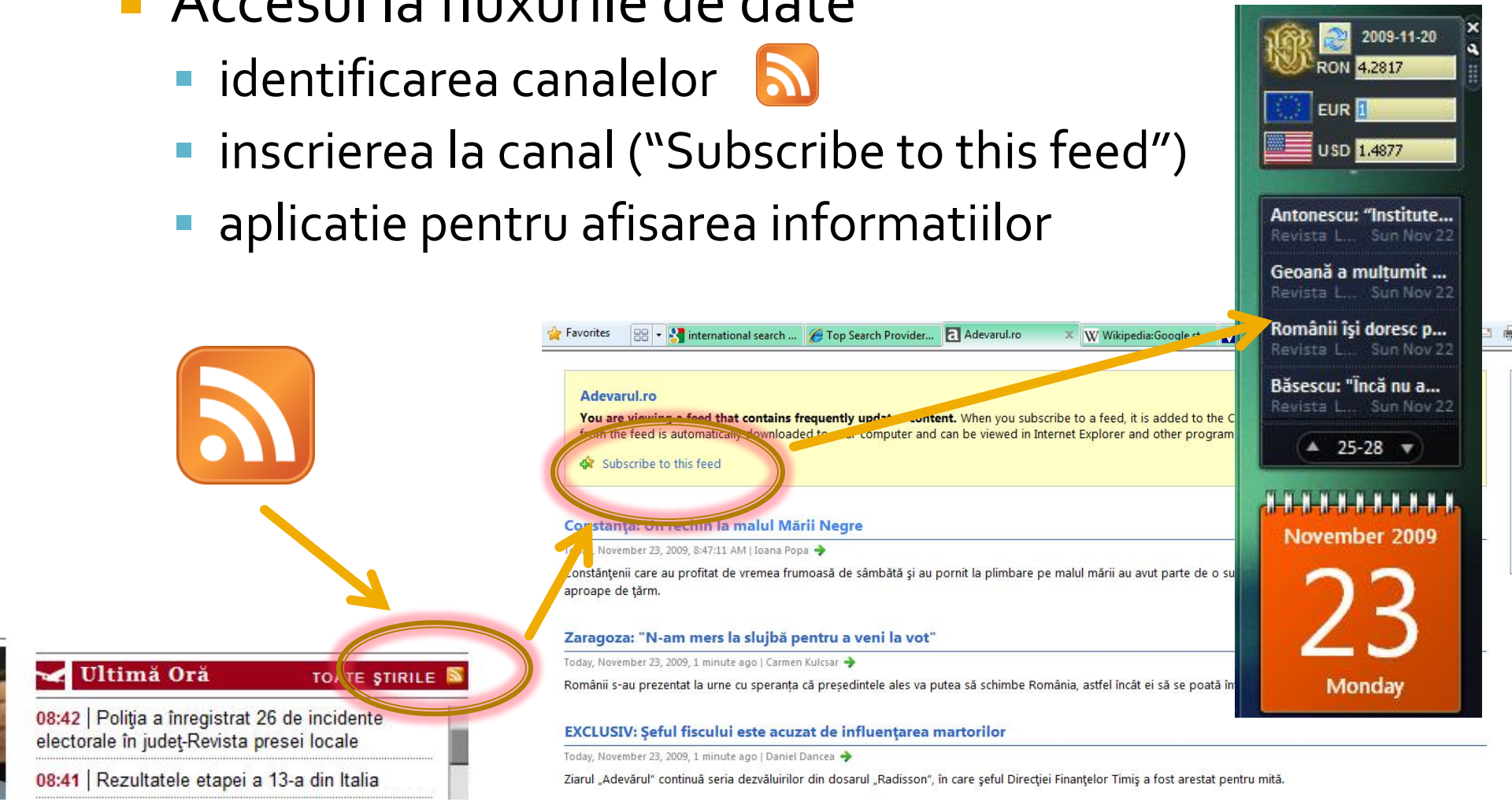


RSS

- RSS – Really Simple Syndication
- Format Web utilizat pentru a face disponibile utilizatorilor sau altor server-e informatii frecvent modificate
  - stiri
  - postari pe forum

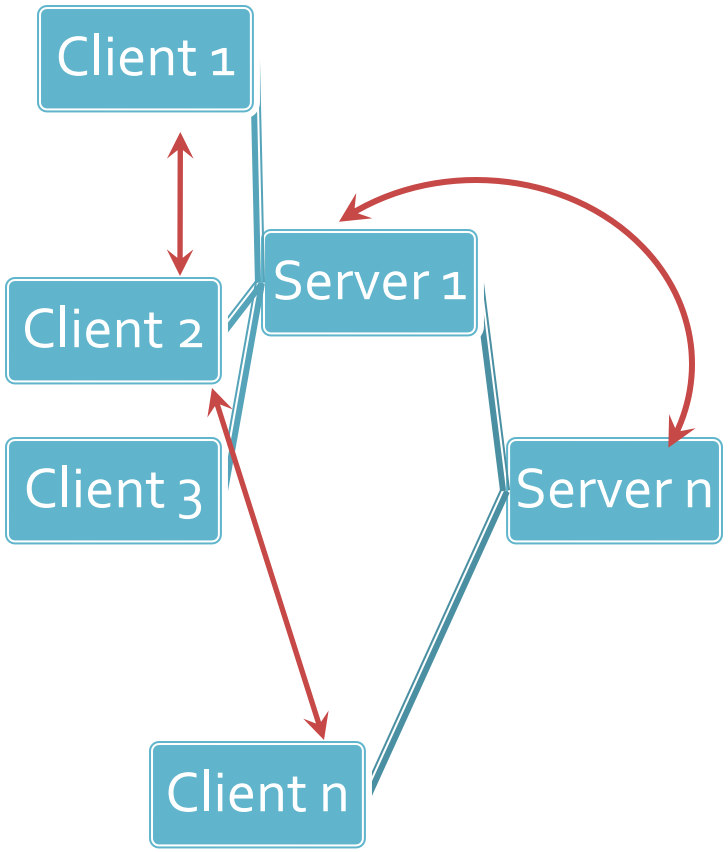
RSS

- Accesul la fluxurile de date
  - identificarea canalelor
  - inscrierea la canal ("Subscribe to this feed")
  - aplicatie pentru afisarea informatiilor



P2P

- P2P – peer to peer
- Modalitate **distribuita** extrem de eficienta de punere in comun si transfer a datelor
  - Datele se gasesc pe calculatoarele client
  - Server-ul mentine o lista
  - Transferul se face direct intre clienti
  - Mai multi clienti simultan
- Aplicatii
  - Kaaza
  - Torrent
  - Emule
  - **Direct Connect**
- Notiuni
  - swarm
  - seed
  - leech
- **Probleme de legalitate**



Retele de socializare

- Rețeaua de socializare Facebook transferă mai multe date decât Google in SUA
- La nivel mondial, activitatea digitală legată de socializare a depăşit activitatea legată de pornografie (lider incontestat până la aceasta dată)
- În SUA, 1 din 8 cupluri căsătorite recent s-au cunoscut pe Internet
- Facebook are mai mulți utilizatori decât populația multor țări de pe glob. "Populația" Facebook ar plasa această rețea pe poziția a 3-a, după China şi India.
- Companiile sunt mai interesate de a obține o imagine bună în rețelele de socializare decât de a fi plasate în top în Google. Din această cauză au aparut şi meserii care constau în frecventarea acestor rețele de socializare pentru a influența aceste imagini

Retele de socializare - Discutii

- Care retea?
- Motive?
- Probleme?

Concepte

- Tipuri de date
- Malware
- Cautare a informatiilor
- Criptare

Tipuri de date

- Web
  - HTML (.html, .htm, .asp, .php)
  - suport – Cascading style sheets, Javascript (.css, .js)
  - imagini
- Date
  - XML, RSS
  - Binare (fisiere oarecare)
  - Aplicatii
    - Java – limbaj interpretat
    - Active X (Internet Explorer)
    - Flash (.swf) – Adobe Flash Player
    - Silverlight (Microsoft)

Tipuri de date

- Documente
  - Portable Document Format (.pdf) – Adobe Reader
  - altele
- Imagini
  - Dimensiunea extrem de importanta (90 -95 % din cantitatea de date web sunt imagini)
  - Formate:
    - jpg – fotografii
    - gif – desene, animatie, transparenta
    - png – vectorial, transparenta

Tipuri de date

- Multimedia – streaming
  - Audio (CD 1411.2kbs, compresat 128-320kbs)
    - mp3 – MPEG 1 Layer 3
    - wma – Windows Media Audio
  - Video
    - avi – Audio Video Interleave
    - wmv – Windows Media Video
    - swf

Malware

- Malicious Software
  - Virus
    - cod executabil
    - reproducere si distributie daca e lansat in executie
  - Worm
    - reproducere si distributie prin transmisie activa prin retea
  - Profit
    - Spyware: aflare de informatii generale si comunicare pe internet
    - Key logger: informatii confidentiale urmate de furt
    - Dialers: acces nedorit la servicii cu plata
- Firewall si Antivirus active si la zi
- Fara click automat: Think before you click

Criptare

- Hash Value – valoare calculata cu un anumit algoritm
  - Data: 10667; Algoritm Hash: Data x 143; Valoare Hash:1525381
  - Daca stiu algoritmul si valoare Hash pot afla datele
- Sisteme de criptare
  - simetrice – aceeasi cheie utilizata la criptare/decriptare si expeditor/destinatar
  - asimetrice
    - cheie publica
    - cheie privata

Criptare

- chei asimetrice
  - cheie publica
    - a destinatarului – la criptare
    - a expeditorului – la verificarea semnaturii digitale
  - cheie privata (~ 3 ori)
    - a destinatarului – la decriptare
    - a expeditorului – la semnare digitala
- exemplu: A trimite un mesaj lui B
  - B isi face cunoscuta **oricui** cheia publica
  - A gaseste cheia publica a lui B (lacat)
  - A cripteaza mesajul cu cheia publica a lui B (cutie)
  - A trimite mesajul criptat pe cai nesigure (posta/prieten)
  - Mesajul poate fi decriptat **numai** cu cheia privata a lui B (cheie)

Coduri simetrice

- OTP – One Time Pad – dovedit matematic sigur (nepractic)
- DES (56b) Data Encryption Standard – 3DES
- AES (128, 192, 256b) Advanced Encryption Standard
- Blowfish
- Twofish (128, 192, 256b)
- Arcfour

Securitate coduri simetrice

- Forta bruta
  - 32 biti – 2^{32} pasi ~10^9 – oricine
  - 40 biti – 2^{40} pasi ~10^{12} – 1 saptamana cu 1 calculator modern
  - 56 biti – Effort substantial
    - retea de calculatoare in comun – cateva luni
    - hardware specializat (scump) – usor: accesibil pentru
      - guverne
      - org. criminale
      - companii mari

Securitate coduri simetrice

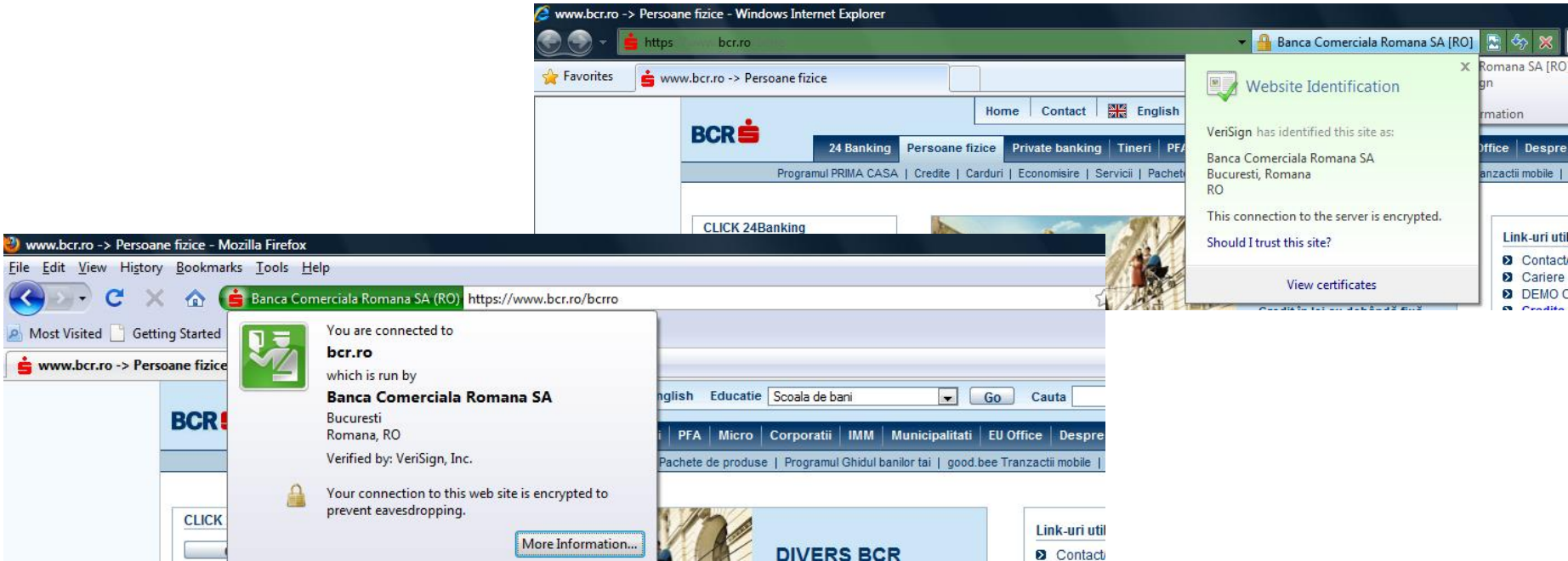
- Forta bruta
  - 64 biti – Pot fi sparte
    - acum – guvernele mari
    - in cativa ani de:
      - guverne mici
      - org. criminale
      - companii mari
  - 80 biti – siguranta pentru cativa ani
  - 128 biti – siguranta pe viitor (10^9 pasi/s – mai mult decat varsta universului)

Coduri asimetrice

- DSS – Digital Signature Standard
- RSA – Rivest, Shamir, Adleman
- Forta bruta
  - 256 biti – usor de spart
  - 512 biti – retea de calculatoare in cateva luni
  - 768 biti – momentan sigure dar nu pe termen lung
  - 1024 biti – sigure pentru cativa ani
  - 2048 – sigure pentru viitor

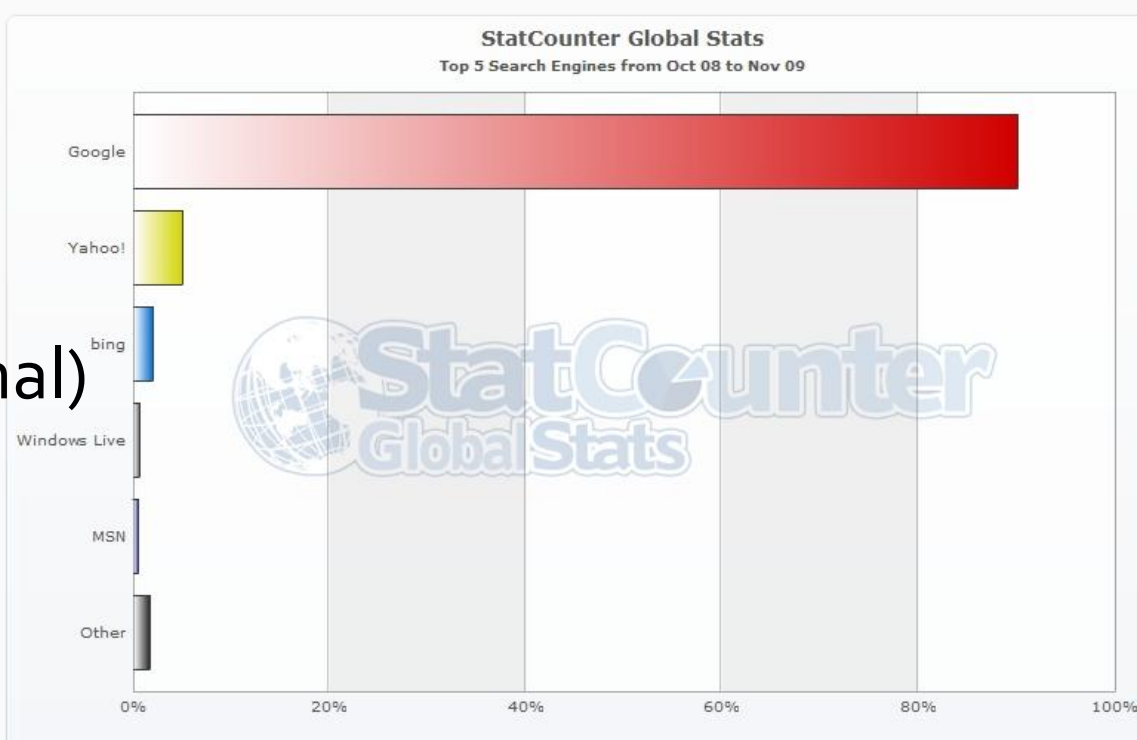
Certification Authorities

- Verisign (si altele)
  - implicit acceptate
  - ~400$/an
- Certificate proprii
  - implicit neacceptate



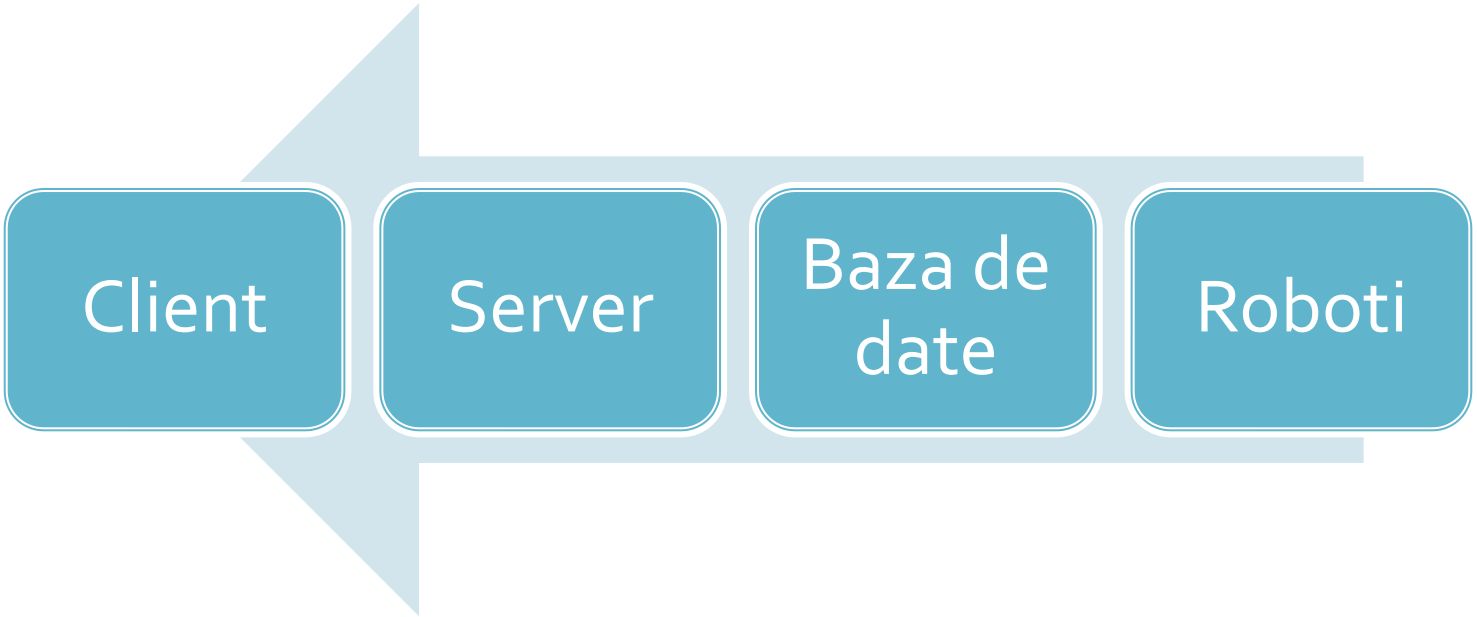
Motoare de cautare

- Motoare de cautare
  - 2008 (SUA)
    - Google (71%)
    - Yahoo (18%)
    - MSN/Live (5%)
  - 2009 (International)
    - Google (89.8%)
    - Yahoo (5.15%)
    - Bing (3.27%)



Motoare de cautare

- SEO
  - Search Engine Optimization



Cautare

- AND
  - Si logic
  - Cuv_1 AND Cuv_2
  - + Cuv_1 +Cuv_2
- OR
  - Sau logic
  - Cuv_1 OR Cuv_2
- NOT
  - negare logica
  - Cuv_1 AND NOT Cuv_2
  - + Cuv_1 -Cuv_2

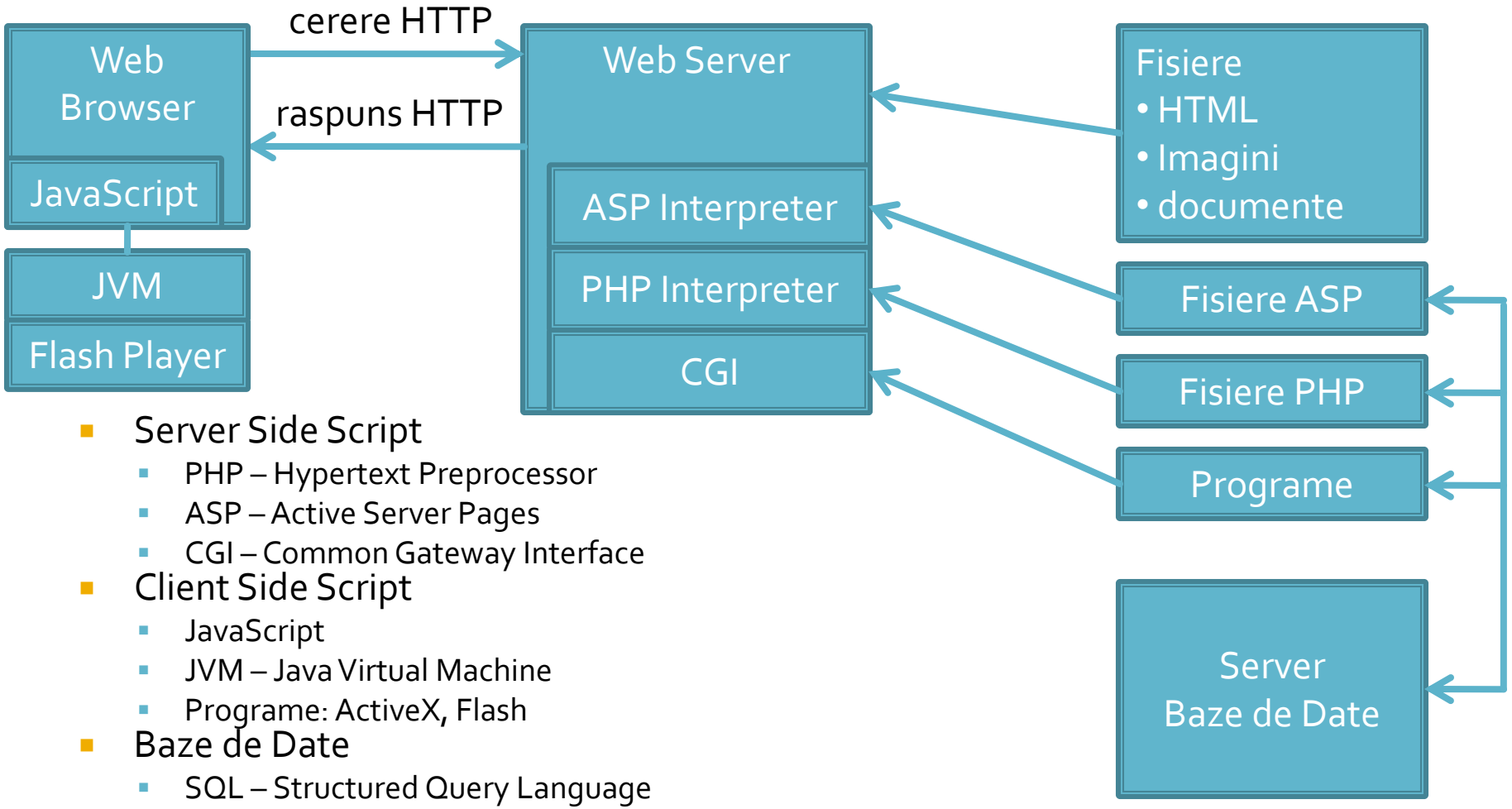
Cautare

- NEAR
  - apropiere in pagina
  - Cuv_1 NEAR Cuv_2
- Fraza
  - “Cuv_1 Cuv_2 …. Cuv_n”
- Operator implicit AND
  - Cuv_1 Cuv_2 = Cuv_1 AND Cuv_2
- Folositi termeni neunivoci
  - ~~film~~ thin film technology
- Incercati sa gasiti un termen care sa fie propriu **numai** informatiei cautate

Cautare exemplu

- Madonna – Like a prayer (versuri)
  - Madonna – 91.500.000
  - Madonna Prayer – 2.880.000
  - +Madonna +Prayer – 2.580.000
  - +Madonna +Prayer –religion – 98.500
  - +Madonna +"Like a prayer" – 818.000
  - +Madonna +"Like a prayer" +lyrics – 144.000
    - **Toate** din primele 10 rezultate contin informatia cautata

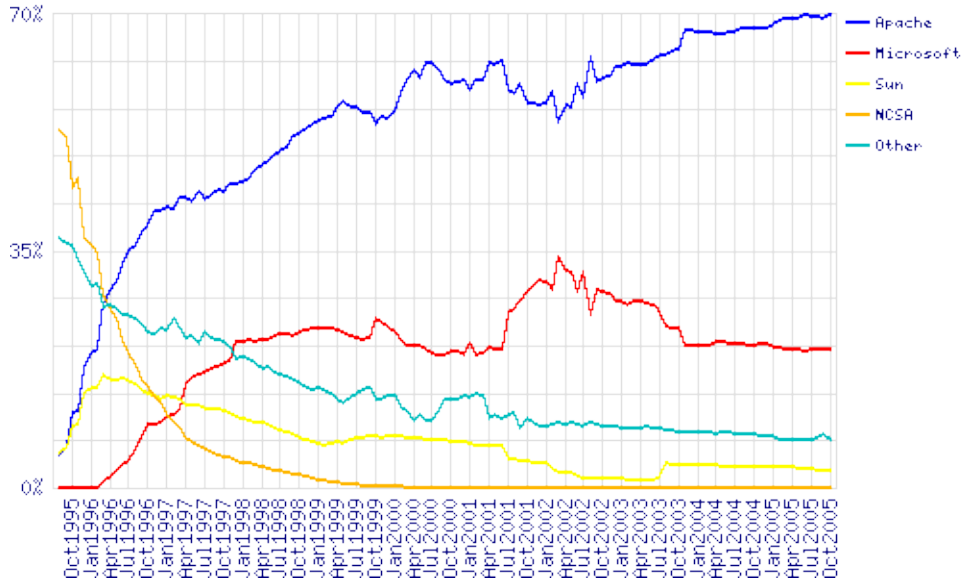
Tehnologia server-elor Web



- Server Side Script
  - PHP – Hypertext Preprocessor
  - ASP – Active Server Pages
  - CGI – Common Gateway Interface
- Client Side Script
  - JavaScript
  - JVM – Java Virtual Machine
  - Programe: ActiveX, Flash
- Baze de Date
  - SQL – Structured Query Language
  - MySql – open Source
  - Microsoft SQL Server
  - Oracle

Tehnologia server-elor Web

- PHP – Hypertext Preprocessor
  - initial – Personal Home Page
  - open source
  - C++
  - Apache
- ASP – Active Server Pages
  - Microsoft
  - VBasic
  - IIS
- Java/JavaScript
  - Sun
  - Masina Virtuala Java



Contact

- Laboratorul de microunde si optoelectronica
- http://rf-opto.etti.tuiasi.ro
- rdamian@etti.tuiasi.ro