Securitatea rețelelor de calculatoare

Laurențiu-Vasile Crețu, Silviu-Laurențiu Vasile

Laborator de finanțe inovative,
13 martie 2025

CUPRINS

- Securizare documente
- Semnătură digitală
- Protejarea documentelor - criptare
- Recuperarea parolelor din documente –decriptare - **tema**
- Rețele de calculatoare
- *Domain Name Service* – **DNS**
- ***Http*** vs ***Https***
- Certificate digitale
- **VPN** (*virtual private network*)
- Concluzii

Securizare documente - metadate

- Istoricul unui document
  - metadatele unui document
  - https://www.metadata2go.com/view-metadata

last_modified_by	vsl
software	Microsoft Office Word
create_date	2024:07:30 20:07:00
modify_date	2024:07:30 20:19:00
security	Locked for annotations
language	en-US
char_count_with_spaces	1138
shared_doc	No

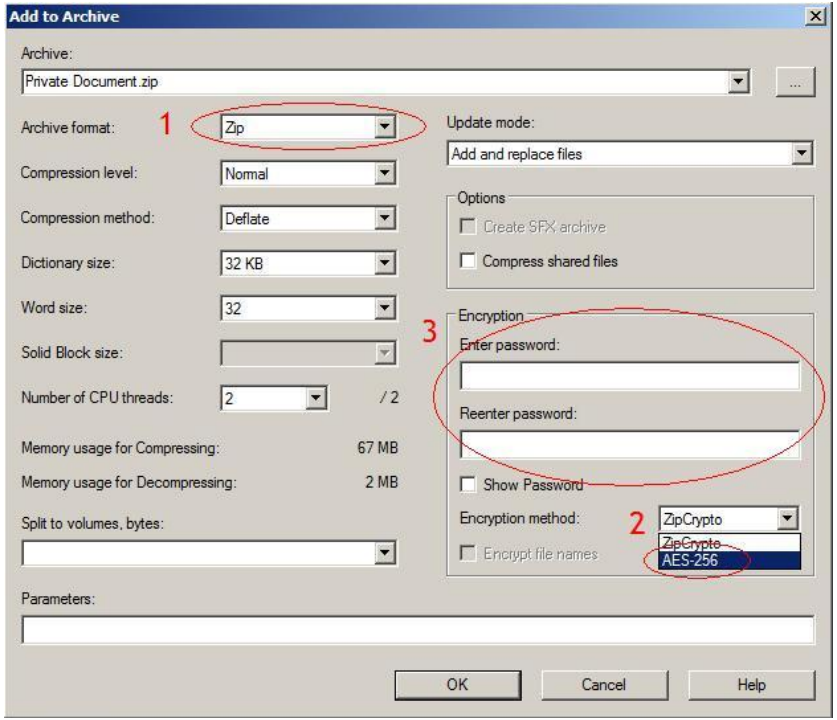
Tipul unui document

- Extensia unui fișier versus signatura unui document
  - cum identific corect tipul unui fișier?
  - https://en.wikipedia.org/wiki/List_of_file_signatures
  - https://sisik.eu/file
  - https://mark0.net/soft-trid-e.html

```
C:\TrID>trid c:\test\doc\lasik_info.doc

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello

Collecting data from file: c:\test\doc\lasik_info.doc
Definitions found: 5702
Analyzing...

 70.7% (.DOC) Microsoft Word document (58000/1/5)
 29.3% (.) Generic OLE2 / Multistream Compound File (24000/1)
```

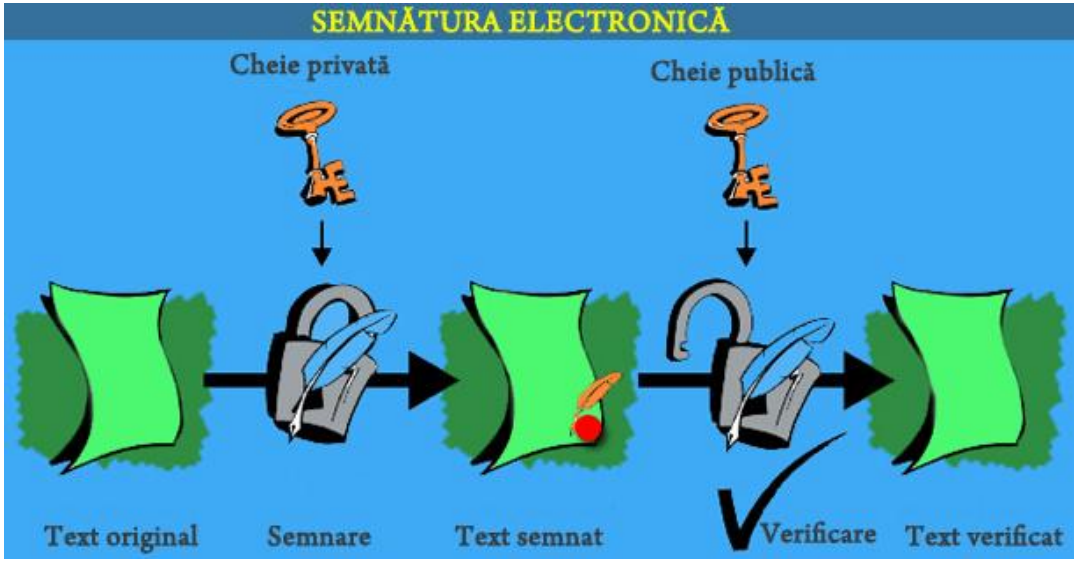
Cum pot “*securiza*” un document

- Documente tip PDF
- Fișiere .XLS, .DOC, .XLSX, .DOCX
- Arhive (.zip, .rar, .tar)



Ce este o semnatură digitală?

- Semnarea unui document
  - generarea/cumpărarea unei semnături digitale
  - exemplu: https://www.digisigner.com/free-electronic-signature/sign-document-online



Multiplicarea unui document electronic

- Pentru a restricționa multiplicarea unui document se folosesc metode de tipul următor:
  - Accesarea conținutului prin intermediul unui program dedicat
  - Utilizarea unei licențe/cod care se validează pe un server extern
  - Blocarea unor opțiuni (copy, printscreen etc.)
  - Adăugarea unui watermark (exemplu: https://tools.pdf24.org/en/add-watermark)
  - Criptarea conținutului
  - etc ...

Documente electronice unice

- Ce metode pot utiliza pentru a realiza o legătură incontestabilă între cel care produce/semnează documentul și cel care achiziționează și apoi multiplică un document?
  - Semnez digital documentele pe care le produc
  - Eventual stochez informații despre utilizarea/accesarea documentului
  - Adaug elemente în document care să îmi permită identificarea persoanei care are drept de utilizare asupra documentului
    - https://incoherency.co.uk/image-steganography/
    - https://www.a.tools/Tool.php?Id=100

Tema - recuperare cheie din fișiere criptate

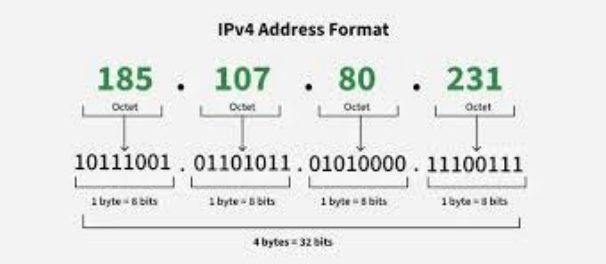
- **Resursă: *https://github.com/laurentiucretu68/ase-cybersecurity***
- Tema abordează problema recuperării unei parole dintr-un document criptat/parolat. În cazul documentelor cu dimensiuni mari, criptarea asimetrică devine ineficientă, fiind preferată criptarea simetrică, astfel în cadrul fișierului este salvat și un *hash* al parolei/cheii utilizate la criptare
- ***Exemple programe utile:***
  - John the Ripper
  - Hashcat
- **Temă**: utilizați "*John the Ripper*" pentru a recupera parola unei arhive de tip .zip
- **Scenariu**:
  - ✓ fiecare participant descarcă fișierul asociat **N.zip**
  - ✓ parola arhiva (**N.zip**) => un cuvânt din textul (**N_raw.txt**)
  - ✓ completează formularul până la data de **19.03.2025** (inclusiv)

Rețele de calculatoare - definiții

- Adresă IP: *Adresa logică asociata unui device (asociem un ip unui device pentru a asigura schimbul de mesaje)*
- PROTOCOL: *set de reguli şi convenţii cu ajutorul căruia se realizează comunicarea într-o reţea (determină formatul, timpul, secvenţele şi controlul erorilor în comunicarea de date) – cel mai comun Internet Protocol (IP)*
- *Alocarea adreselor IP nu este arbitrară; ea se face de către organizații însărcinate cu distribuirea de spații de adrese (RIPE – Europa - https://www.ripe.net)*

➢ *Locația unui IP: https://www.iplocation.net/*

➢ *Detalii IP: https://search.censys.io/*



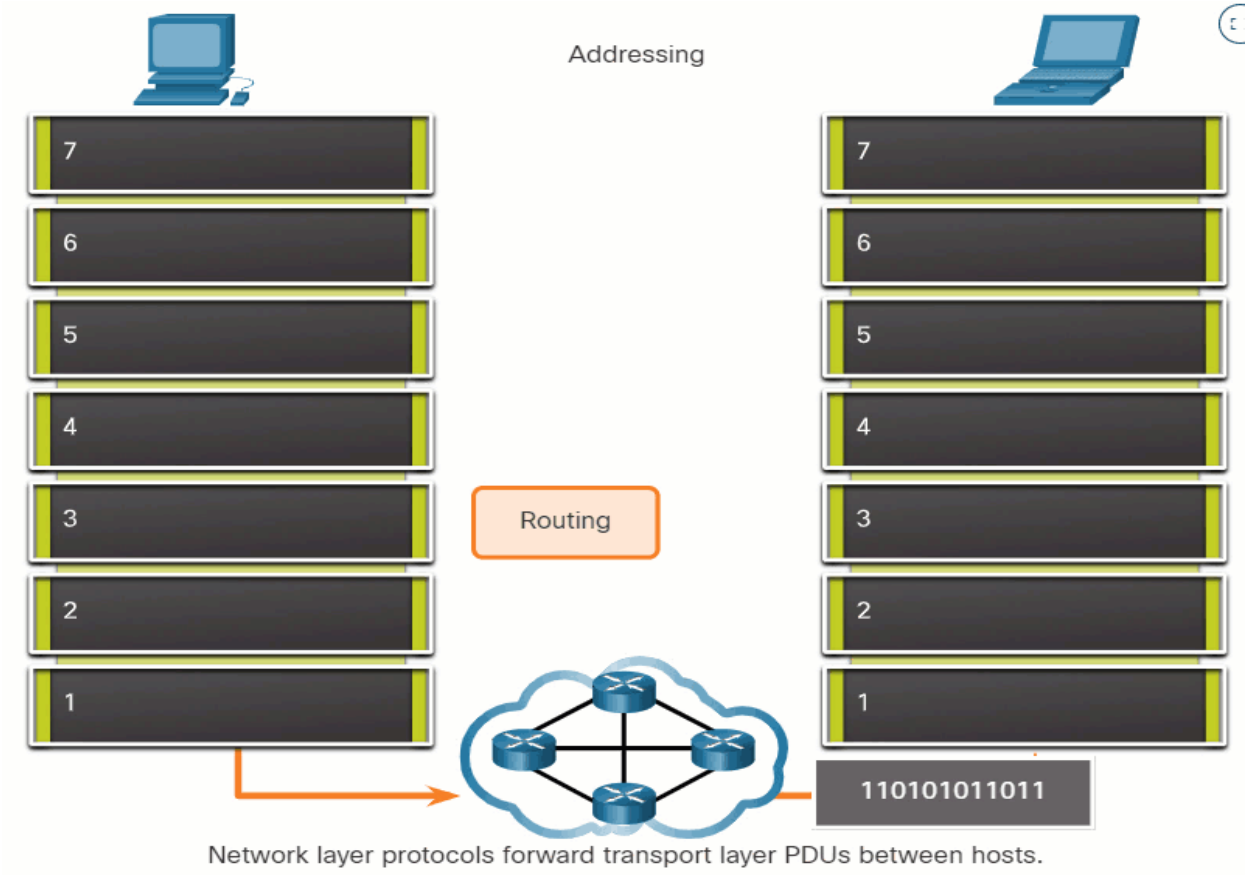
- PROTOCOLUL IP

✓ Este proiectat sa fie folosit peste o retea dinamica

✓ Nu trebuie sa depinda de un nod central si nu trebuie sa depinda de alte resurse

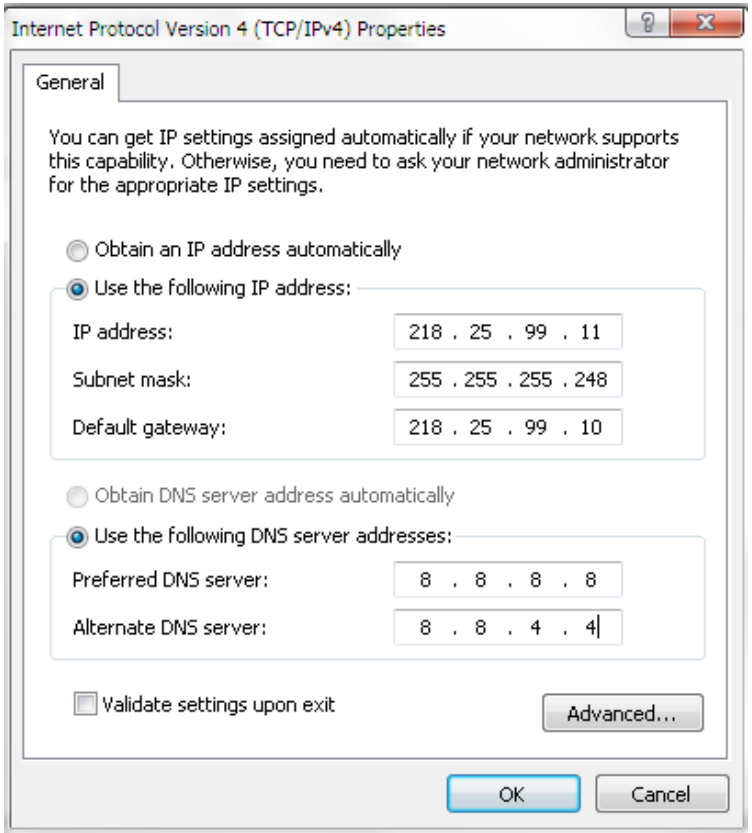
✓ Este un protocol în care fiecare pachet contine sursa si destinatia

Cum funcționează? OSI - *Open Systems Interconnection*



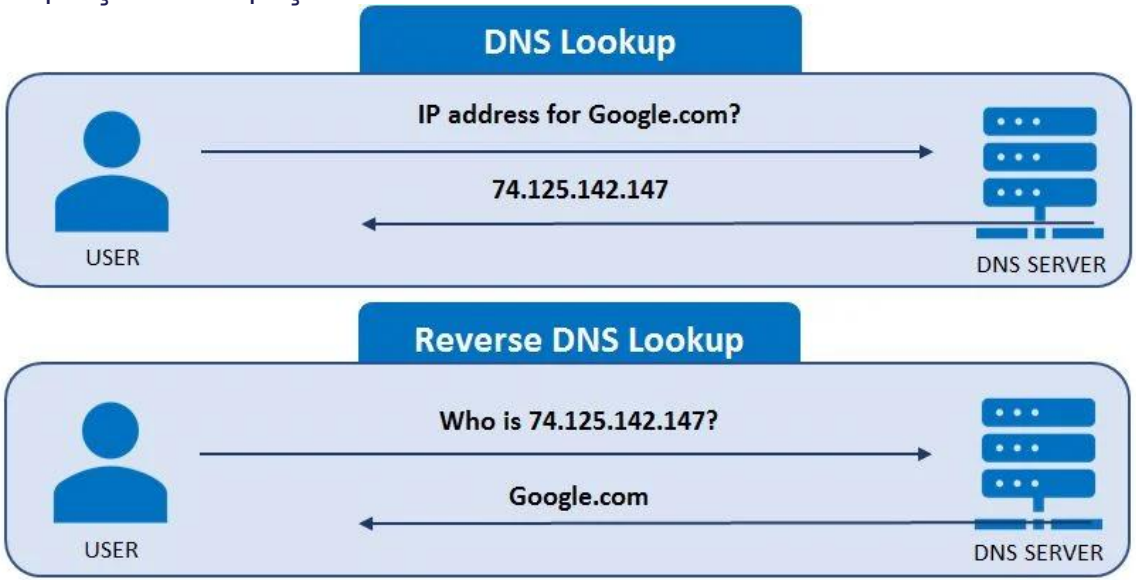
Configurarea unui echipament

- IP address
- Subnet mask
- Default gateway
- DNS server address
  - Google: 8.8.8.8; 8.8.4.4
  - CloudFlare: 1.1.1.1; 1.0.0.1



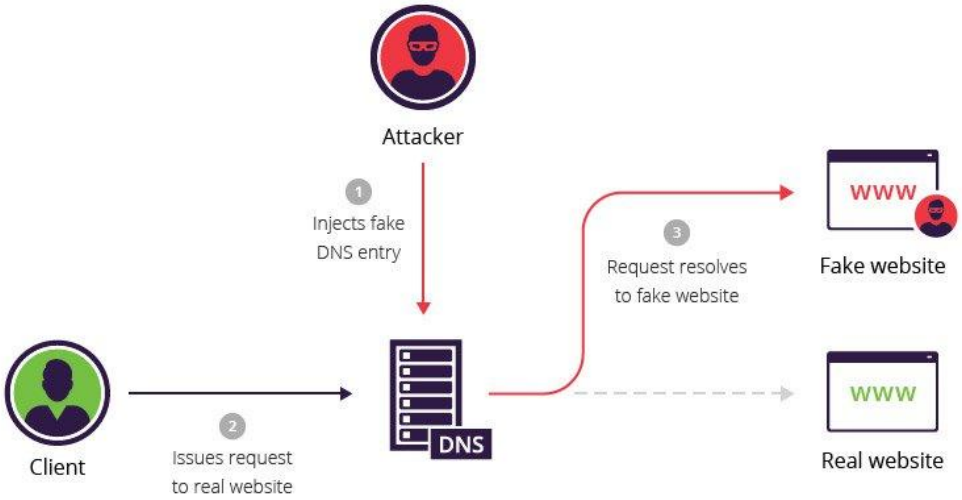
Domain Name Service – DNS

- Protocol client – server
- Spaţiul de nume DNS – structură logică arborescentă
- Fiecare nod reprezintă un domeniu = porţiune din spaţiul de nume
- Rotld.ro => domenii .ro
- DNS server address
  - Google: 8.8.8.8; 8.8.4.4
  - CloudFlare: 1.1.1.1; 1.0.0.1



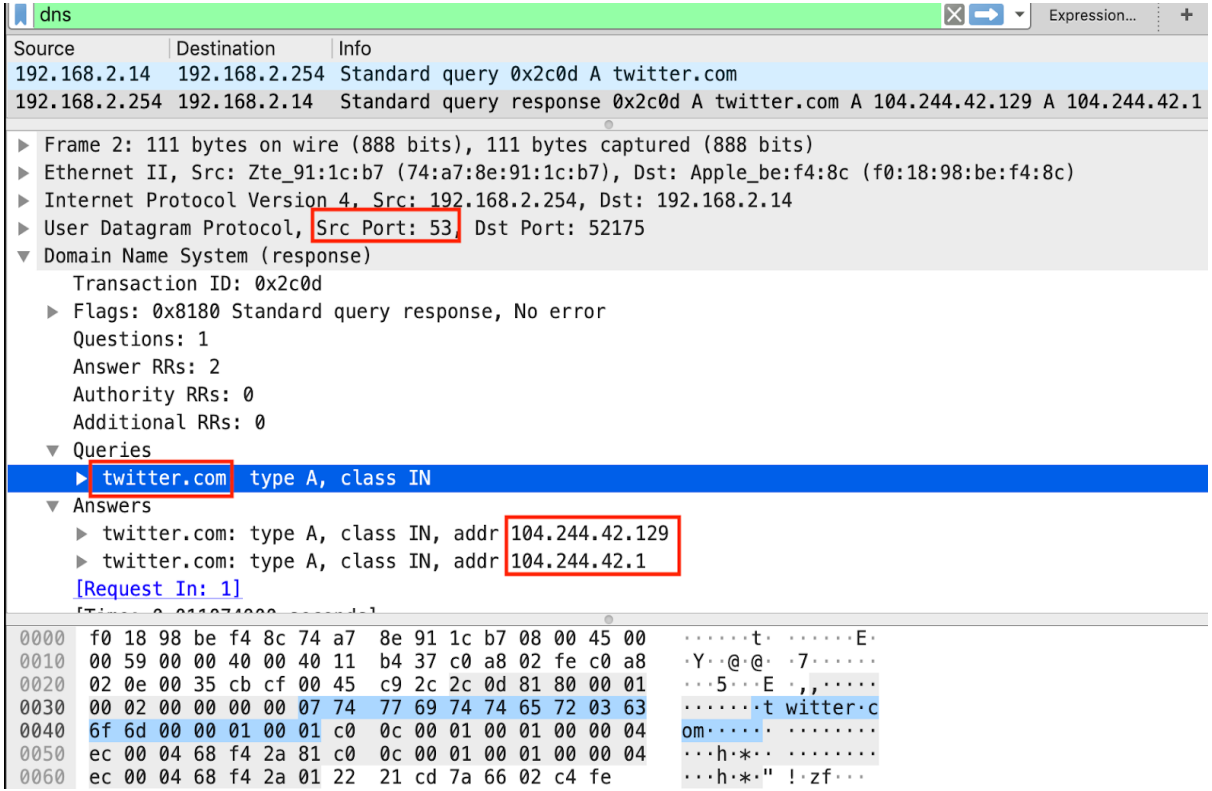
DNS spoofing

- o metodă utilizată pentru a modifica adresele serverelor DNS pe care le folosește utilizatorul
- un atacator poate modifica adresele IP allocate unor domenii prin adaugarea de intrari false in adresele DNS ale victimei; in acest fel puteți fi redirecționat către o altă pagină complet diferită
- DNS server address recomandate
  - Google: 8.8.8.8; 8.8.4.4
  - CloudFlare: 1.1.1.1; 1.0.0.1



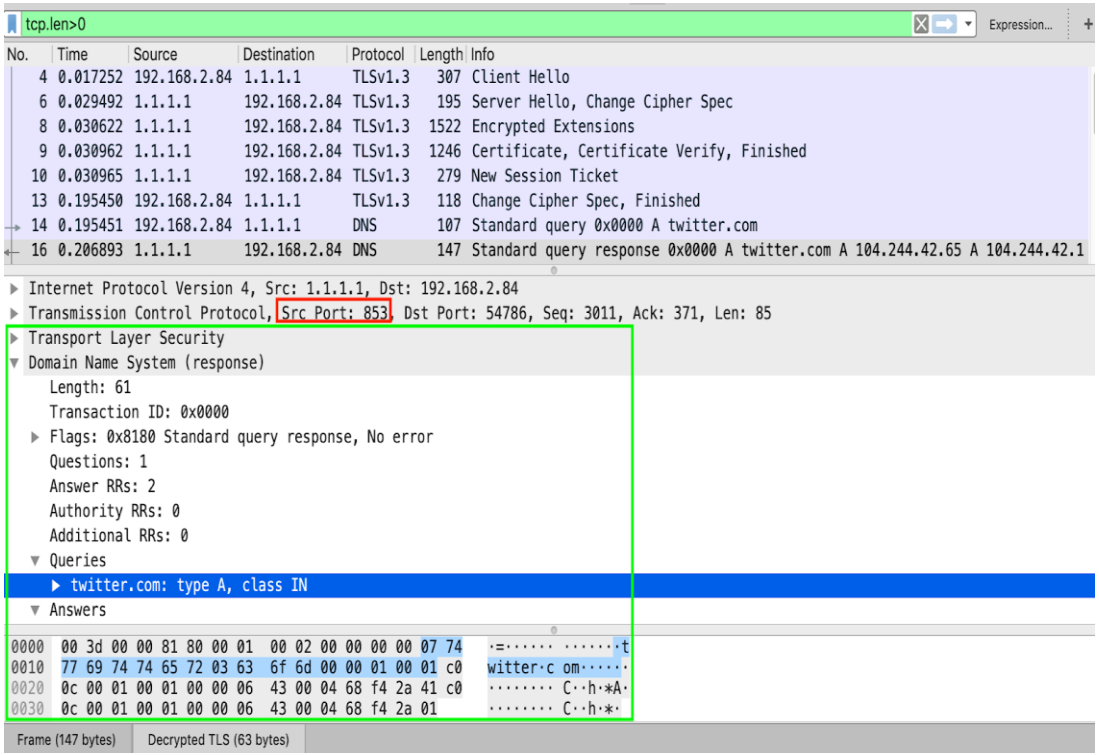
DNS Encryption (1)

- DNS over TLS (DoT)
- DNS over HTTPS (DoH)



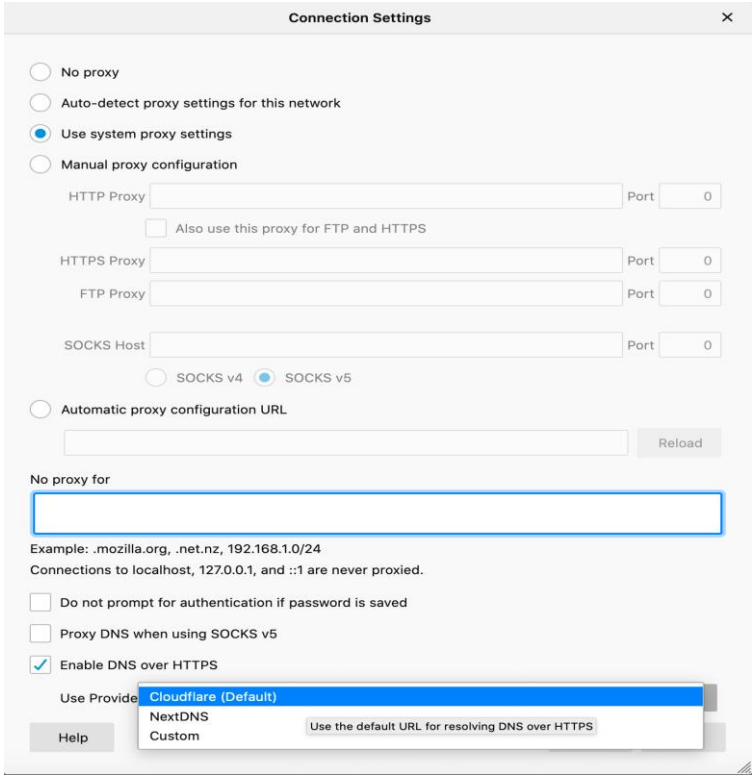
DNS Encryption (2)

- DNS over TLS (DoT)
- DNS over HTTPS (DoH)



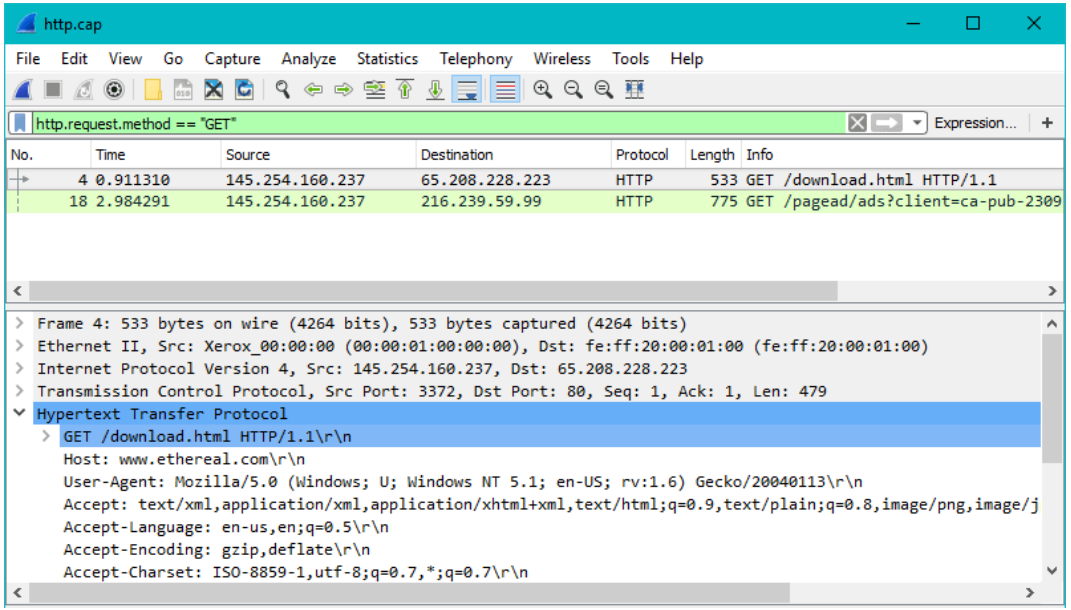
DNS Encryption (3)

- **Mozilla Firefox**
  - menu > **Settings**.
  - **General** > **Network Settings**.
  - **Settings** > **Enable DNS over HTTPS**



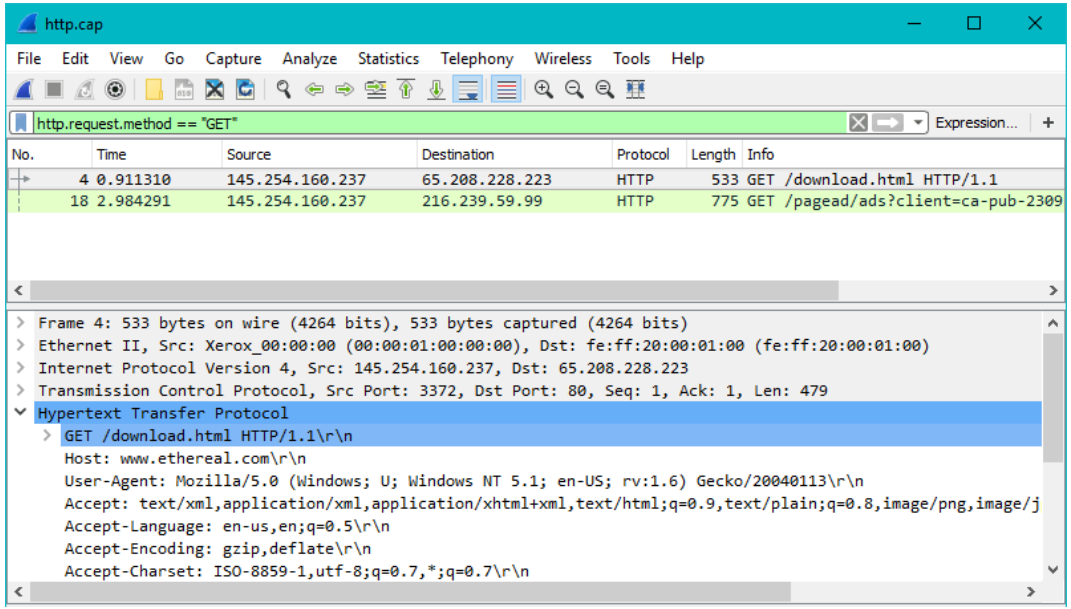
Http vs Https

- Hypertext Transfer Protocol
- Face parte din stiva de protocoale TCP/IP (port 80)
- Original a fost conceput numai pentru transferul paginilor HTML
- În prezent este folosit pentru o gamă largă de tipuri de date
- Unul dintre cele mai folosite protocoale
- Forma criptată https (443)



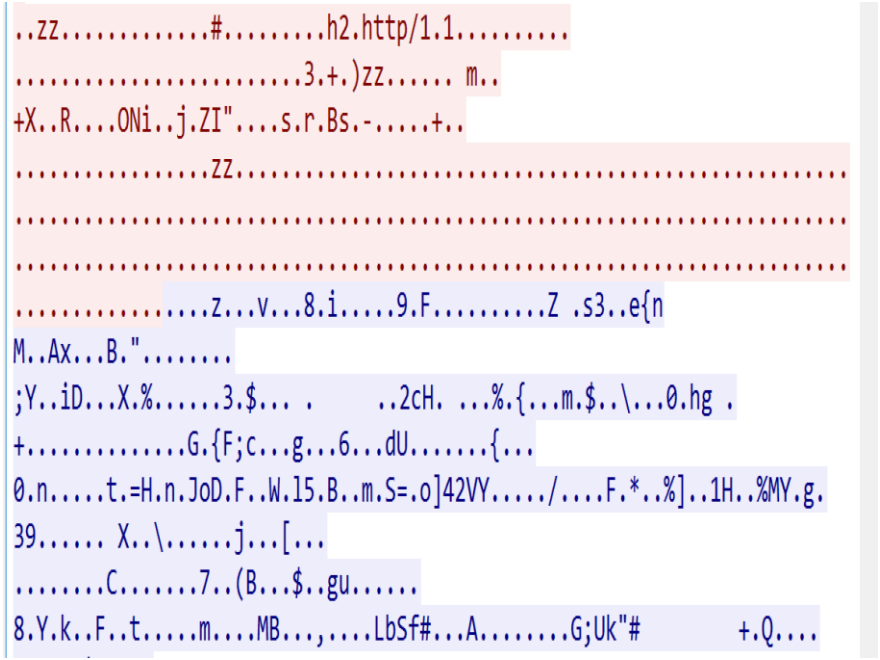
Http vs Https

- Hypertext Transfer Protocol
- Face parte din stiva de protocoale TCP/IP (port 80)
- Original a fost conceput numai pentru transferul paginilor HTML
- În prezent este folosit pentru o gamă largă de tipuri de date
- Unul dintre cele mai folosite protocoale



Http vs Https

- Forma criptată https (443)



Https vulnerabil?

- Aprilie 2014:

- In data de 7 aprilie 2014 a fost facuta publica o vulnerabilitate majora in OpenSSL, populara librarie de functii criptografice open-source. Vulnerabilitatea are codul CVE-2014-0160 si este denumita public Heartbleed.

- Vulnerabilitatea permite unui atacator sa obtina portiuni de date din memoria server-ului web. Chiar daca Heartbleed nu este un defect al certificatelor SSL sau protocolul TLS, exploatarea acestei brese de securitate poate duce la compromiterea cheii private, parolelor sau ale altor date sensibile

- Testare domeniu on-line: https://www.ssllabs.com/ssltest/analyze.html

Detalii certificate https

- ismma.ro

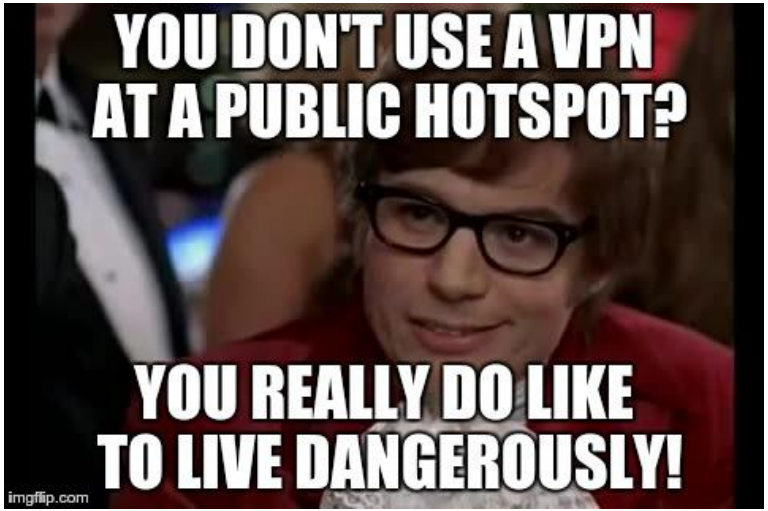
Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	csm.ro Fingerprint SHA256: 56e822491f1e787e4c57ed503a5322cff86645b536f83dfaaf7b31f0337ff83c Pin SHA256: w1xpEFUzSPXLB9dltLcBDwyZyzIVvRe5hcFEUcsaI5U=
Common names	csm.ro
Alternative names	csm.ro ismma.ro mail.csm.ro mail.ismma.ro www.csm.ro www.ismma.ro www.mail.csm.ro www.mail.ismma.ro
Serial Number	04b0e21027d56494a4df05ecc383ff2825ad
Valid from	Tue, 03 Jan 2023 08:56:18 UTC
Valid until	Mon, 03 Apr 2023 08:56:17 UTC (expires in 20 days, 11 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

VPN (virtual private network)

Este necesară utilizarea unei soluții de tip VPN?



Ce este un VPN?

- Un VPN este o rețea privată punct la punct peste o rețea publică (ex: Internet)
- Un VPN nu garantează neapărat confidențialitatea traficului
- Pot fi folosite folosite metode criptografice
- Un VPN devine un tunel prin care sunt transportate date criptate
- Poate asigura și autentificarea sursei datelor

Beneficiile rețelelor virtuale - VPN

- **Cost redus**

VPN-urile nu au nevoie de legături fizice dedicate și pot funcționa fără hardware specializat

- **Securitate crescută**

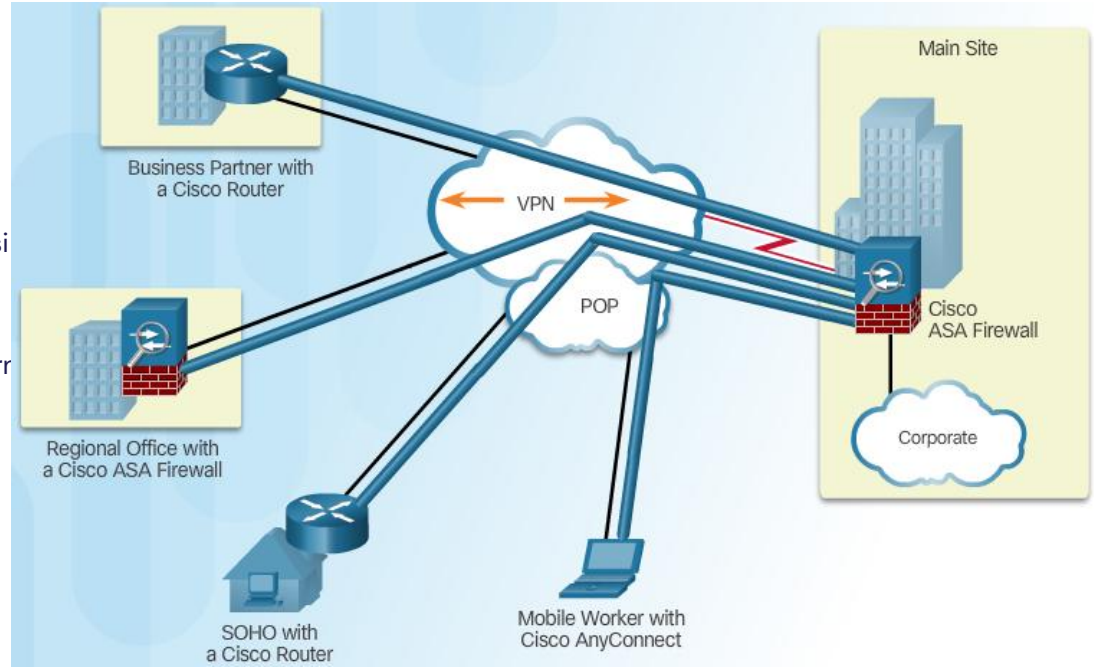
VPN-urile folosesc protocoale sigure de criptare și autentificare

- **Scalabilitate**

VPN-urile folosesc infrastructura existentă în Interr
Adăugarea de utilizatori și rețele este ușoară

- **Compatibilitate**

VPN-urile pot traversa medii și rețele diferite



Tunelare: încapsulare

- **Orice tehnologie de VPN se bazează pe tunelare**

Tunelarea presupune încapsularea cu încă un antet la nivelul la care se contruiește tunelul

Exemplu: tunelul *IPIP*

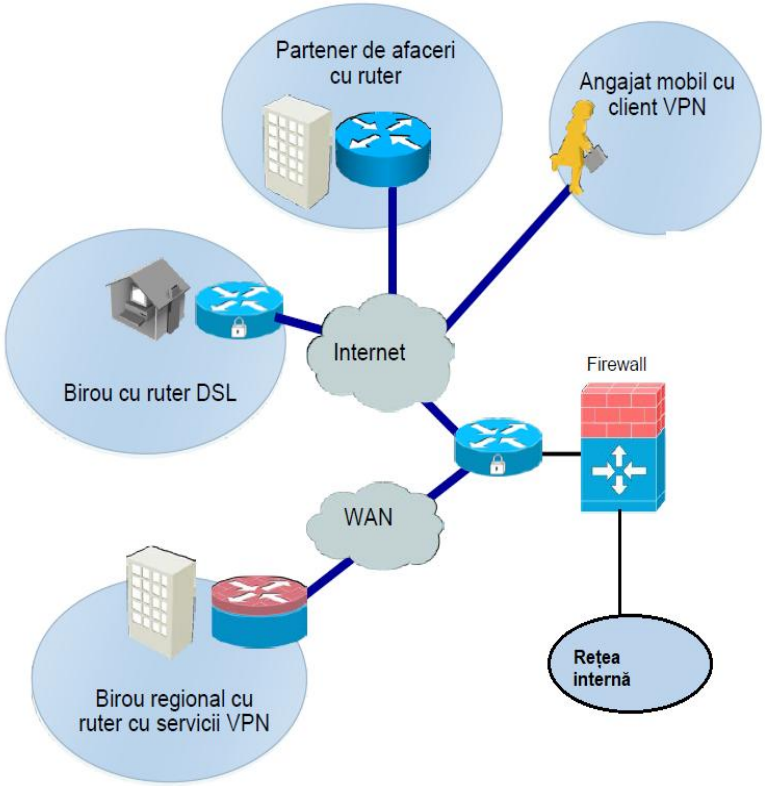
- *Folosit când rețeaua sursă sau destinație nu este cunoscută în tabela de rutare a unui ruter intermediar*

- *Antetul IP original nu este cunoscut ruterelor intermediare!*

Clasificarea soluțiilor VPN

Virtual: Informația într-o rețea privată este transportată peste o rețea publică

Privat: Traficul poate fi criptat pentru a asigura confidențialitate



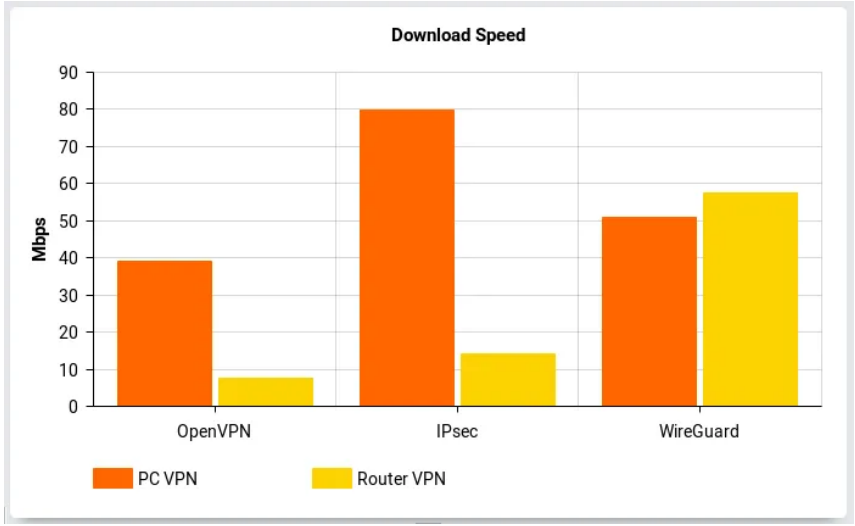
Clasificarea soluțiilor VPN

- Un VPN este un tunel care interconectează două puncte peste o rețea publică
- Pentru a transporta datele la destinație, un antet este adăugat la toate pachetele ce trec prin tunel (oferă toate beneficiile unui VPN)
- Antetul conține și informațiile de adresare ce permit pachetelor să ajungă la destinație
- VPN-urile pot fi implementate la nivelurile 2, 3 și 5 în stiva OSI
- Este prezentat un model de nivel 3

Comparație protocoale VPN

📊 Comparație protocoale VPN

Protocol	Securitate	Viteză	Use Case
OpenVPN	🔒🔒🔒🔒	🐢	Securitate maximă
WireGuard®	🔒🔒🔒	🚀	Dispozitive mobile
IKEv2/IPsec	🔒🔒🔒🔒	🔄	Schimbări rețea



Exemplu traffic (fara VPN)

```
C:\Users\vsl>tracert fmi.unibuc.ro

Tracing route to fmi.unibuc.ro [80.96.21.88]
over a maximum of 30 hops:

  1     6 ms     3 ms     3 ms  192.168.100.1
  2     *        *        *     Request timed out.
  3     7 ms    15 ms     8 ms  172.20.183.5
  4     7 ms     6 ms     8 ms  roedu.interlan.ro [86.104.125.98]
  5    15 ms    10 ms     9 ms  te-4-3.core2.nat.roedu.net [37.128.239.41]
  6    11 ms    11 ms    11 ms  hu-0-2-0-0.core2.buc.roedu.net [37.128.239.102]
  7     9 ms     *        *     po-13.acc1.buc.roedu.net [37.128.232.178]
  8     6 ms     6 ms     6 ms  37.128.224.178
  9     *        *        *     Request timed out.
 10    10 ms     7 ms     8 ms  80.96.21.88

Trace complete.
```

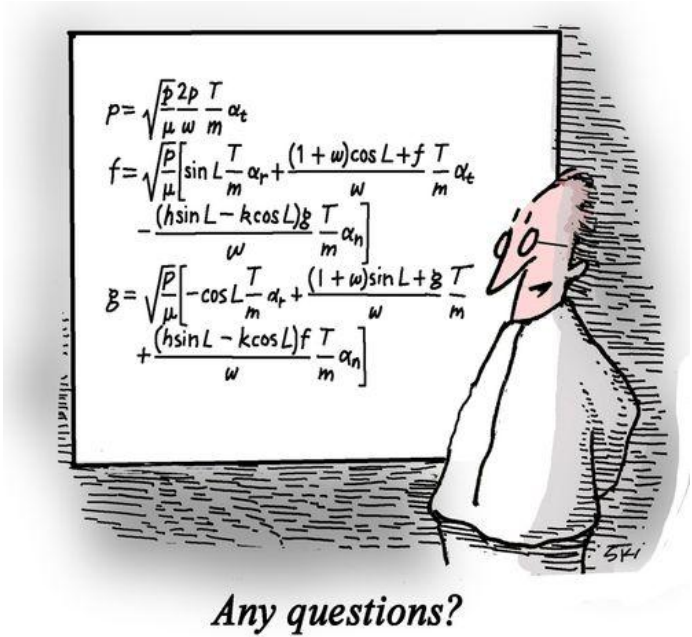
Exemplu trafic (cu VPN)

```
C:\Users\vsl>tracert fmi.unibuc.ro

Tracing route to fmi.unibuc.ro [80.96.21.88]
over a maximum of 30 hops:

  1    14 ms     9 ms     7 ms  192.168.23.1
  2    19 ms    15 ms     9 ms  10.1.32.1
  3     8 ms    15 ms    10 ms  node-bge.pool-1-2.dynamic.totinternet.net [1.2.185.254]
  4     9 ms     9 ms     7 ms  172.20.241.5
  5    10 ms     9 ms    13 ms  10.0.221.41
  6    10 ms     9 ms     7 ms  10.0.200.178
  7     8 ms     8 ms     8 ms  172.20.241.2
  8    11 ms     8 ms    11 ms  10.255.10.1
  9     9 ms     8 ms     8 ms  80.96.21.88

Trace complete.
```

Concluzii

- Autentificare, transmitere formulare => strict https;
- Verificati certificatele utilizate pentru criptarea traficului;
- Evitati conectarea la retele publice (open);
- Limitati utilizarea retelelor wireless;
- Plata on-line doar prin intermediul unor operatori recunoscuti (diferite banci, euplatesc, mobilpay etc), poate carduri dedicate/speciale (plata in 2 pasi);
- Nu accesati link-uri, atasamente ale unor mail-uri care nu par legitime;
- Verificati detaliile (mesajul original) pentru mesajele suspecte;
- Incercati utilizarea unei solutii de tip VPN.

Vă mulțumim!


$$p=\sqrt{\frac{p}{\mu}\frac{2p}{w}}\frac{T}{m}\alpha_t$$
$$f=\sqrt{\frac{p}{\mu}}\left[\sin L\frac{T}{m}\alpha_r+\frac{(1+w)\cos L+f}{w}\frac{T}{m}\alpha_t - \frac{(h\sin L-k\cos L)g}{w}\frac{T}{m}\alpha_n\right]$$
$$g=\sqrt{\frac{p}{\mu}}\left[-\cos L\frac{T}{m}\alpha_r+\frac{(1+w)\sin L+g}{w}\frac{T}{m} + \frac{(h\sin L-k\cos L)f}{w}\frac{T}{m}\alpha_n\right]$$
Any questions?


End-user Education
Application Security
IOT Security
Information Security
Cyber Security
ICT Security
Network Security
Internet Security
Operational Security