

Securitatea rețelor 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 - metadata

- ❑ Istoricul unui document

- ❑ metadatale 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 semnatura 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
```

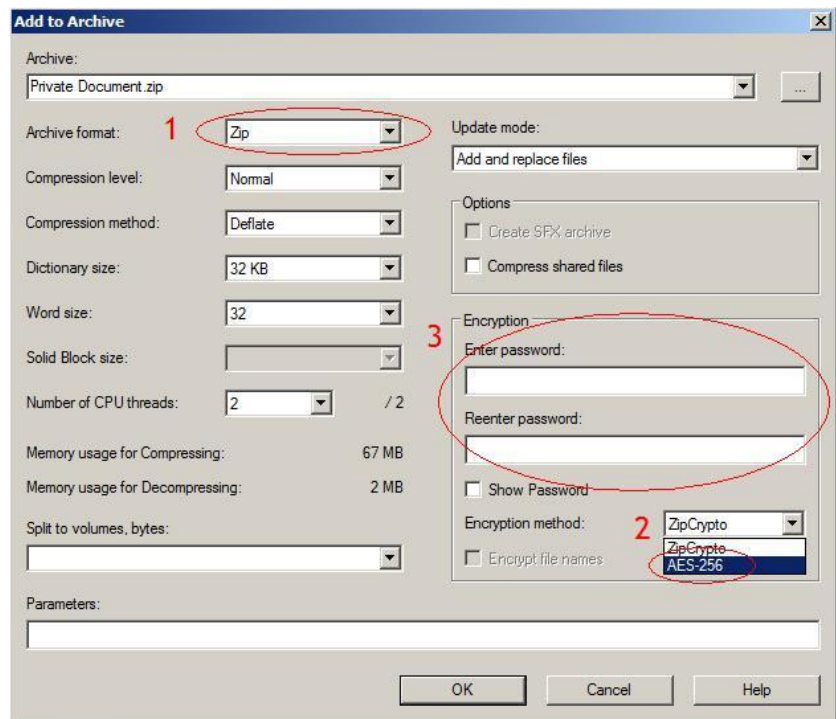
```
Analyzing...
```

```
70.7% (.DOC) Microsoft Word document (58000/1/5)
```

```
29.3% (.) Generic OLE2 / Multistream Compound File (24000/1)
```

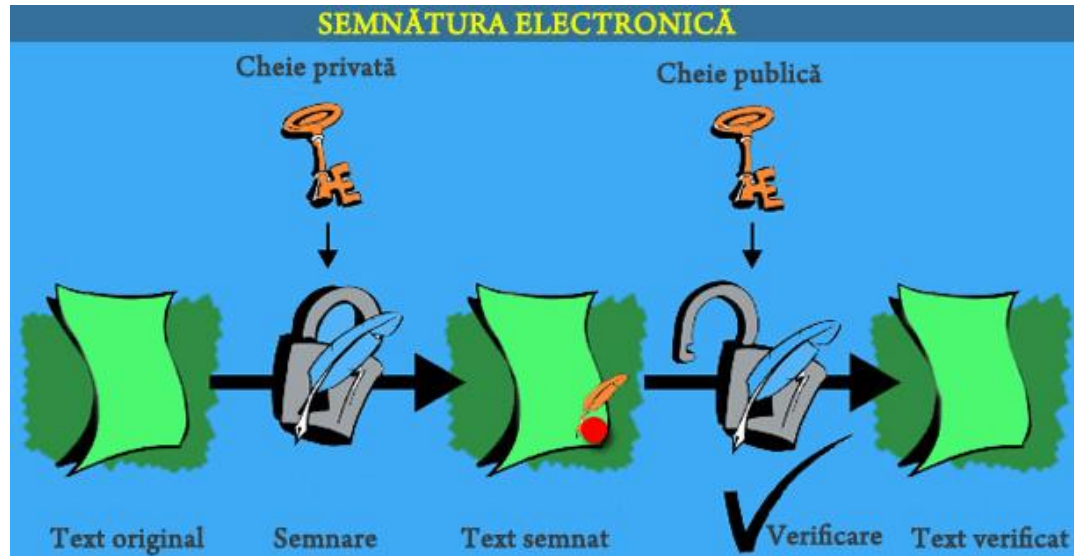
Cum pot “*securiza*” un document

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



Ce este o semnătură 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
 - ❑ Aaug 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 inefficientă, 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](#)

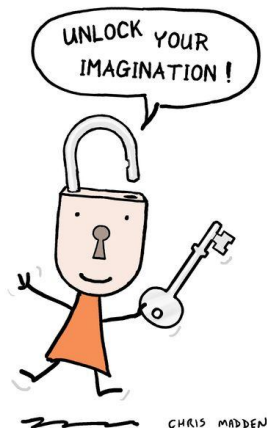


- ❑ [Hashcat](#)

- ❑ **Temă:** utilizați "John the Ripper" pentru a recupera parola unei arhive de tip .zip

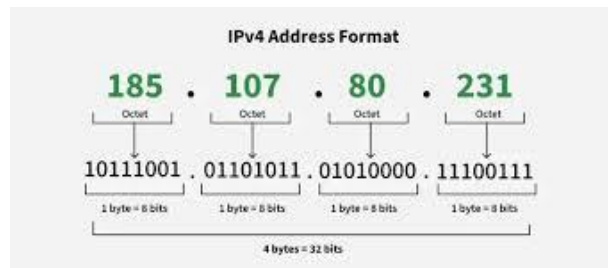
- ❑ **Scenariu:**

- ✓ 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)

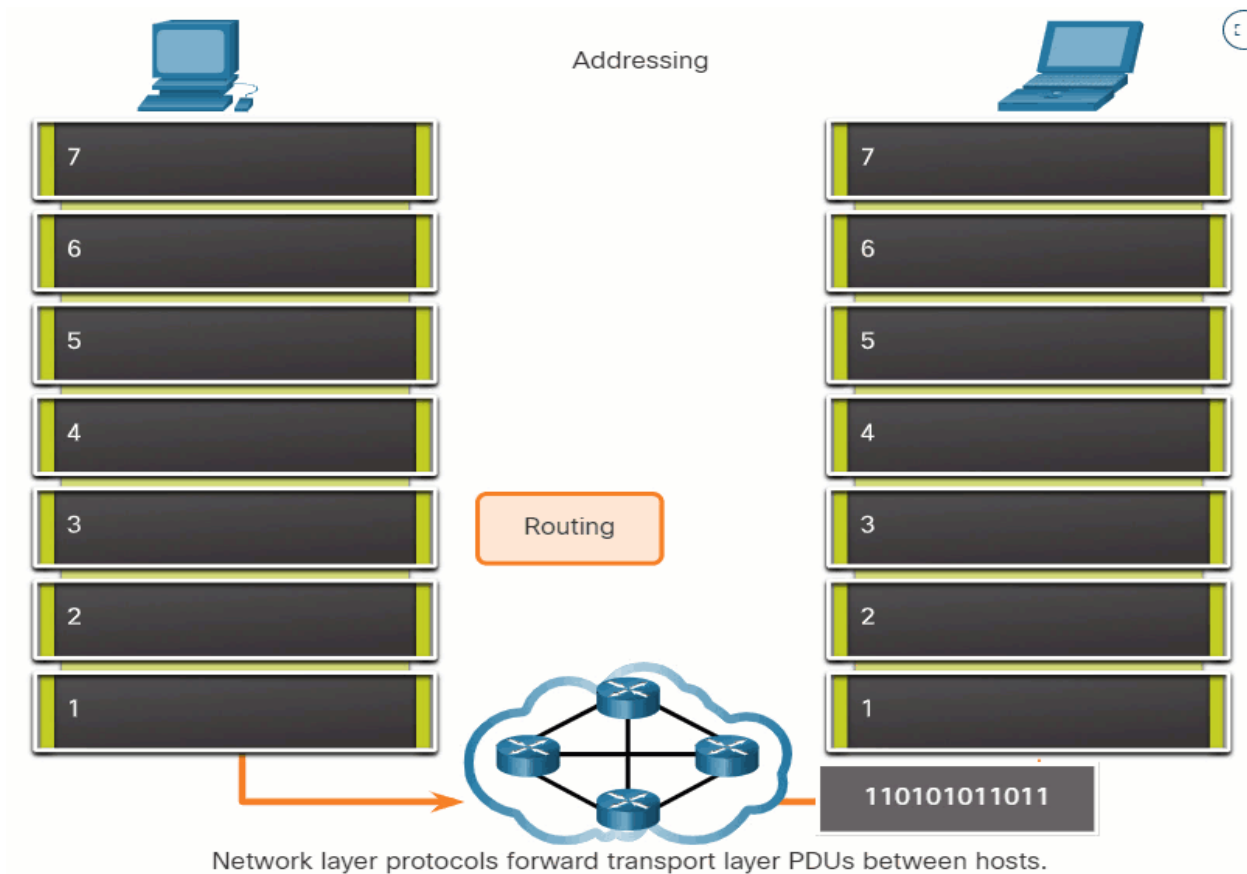


Rețele de calculatoare - definiții

- ❑ Adresă IP: Adresa logică asociată unui device (asociem un ip unui device pentru a asigura schimbul de mesaje)
- ❑ PROTOCOL: set de reguli și convenții cu ajutorul căruia se realizează comunicarea într-o rețea (determină formatul, timpul, secvențele și 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 să fie folosit peste o rețea dinamică
- ✓ Nu trebuie să depindă de un nod central și nu trebuie să depindă de alte resurse
- ✓ Este un protocol în care fiecare pachet conține sursa și destinația

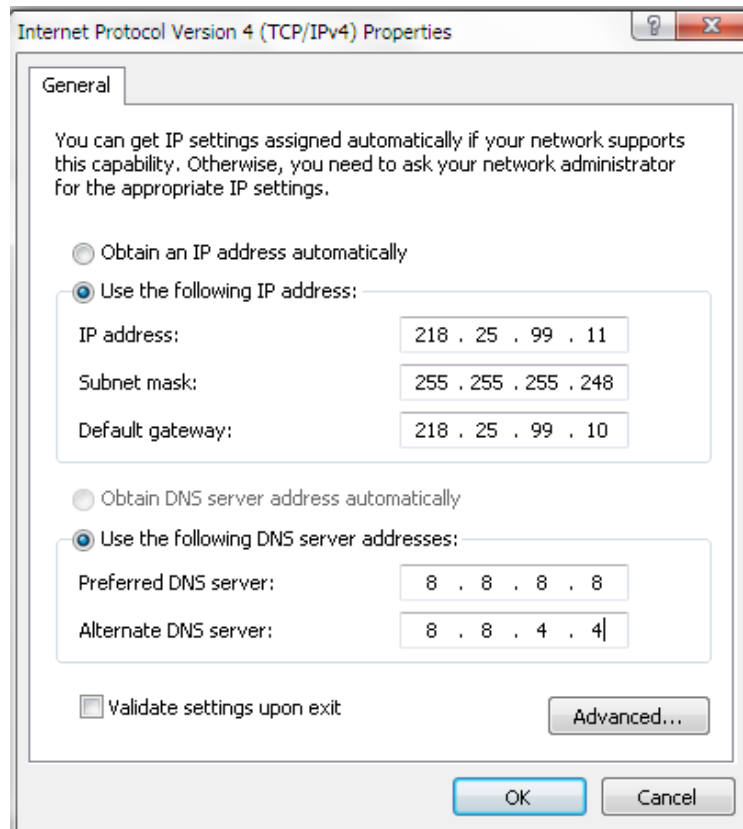


Cum funcționează? OSI - *Open Systems Interconnection*



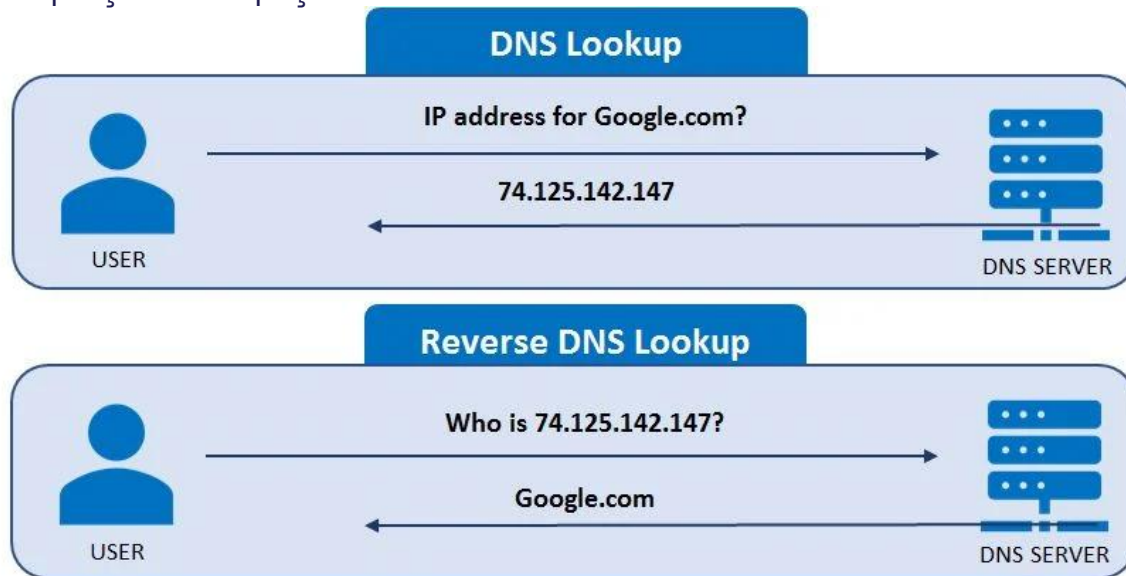
Configurarea unui echipament

- ☐ 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



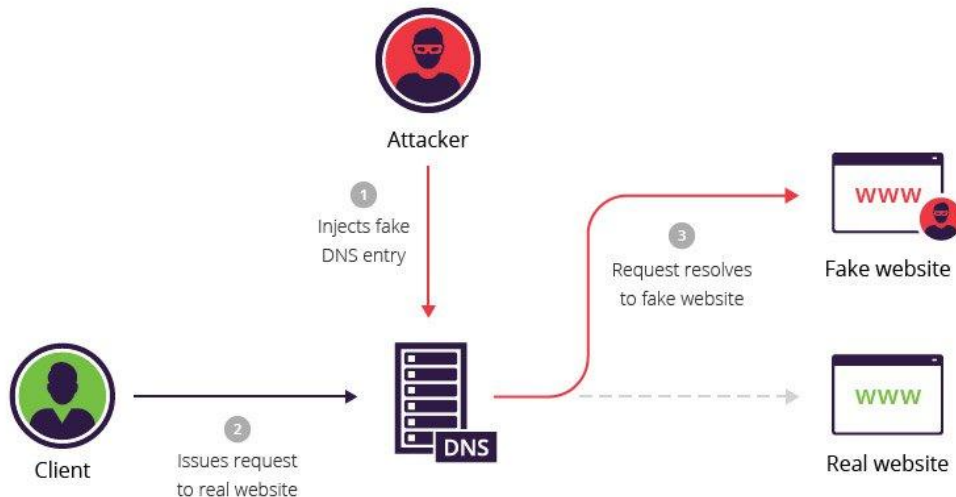
Domain Name Service – DNS

- ❑ Protocol client – server
- ❑ Spațiul de nume DNS – structură logică arborescentă
- ❑ Fiecare nod reprezintă un domeniu = porțiune din spațiul 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)

The image shows a Wireshark packet capture of a DNS response. The packet list pane at the top shows two packets: a standard query from 192.168.2.14 to 192.168.2.254, and a standard query response from 192.168.2.254 to 192.168.2.14. The packet details pane shows the structure of the response, including the Ethernet II header, IP header (Src Port: 53), and the Domain Name System (response) section. The transaction ID is 0x2c0d. The flags indicate a standard query response with no error. The questions section shows a query for twitter.com, type A, class IN. The answers section shows two answers for twitter.com, type A, class IN, with IP addresses 104.244.42.129 and 104.244.42.1. The packet bytes pane at the bottom shows the raw data of the packet, with the domain name twitter.com and the IP addresses 104.244.42.129 and 104.244.42.1 highlighted in blue.

dns

Source	Destination	Info
192.168.2.14	192.168.2.254	Standard query 0x2c0d A twitter.com
192.168.2.254	192.168.2.14	Standard query response 0x2c0d A twitter.com A 104.244.42.129 A 104.244.42.1

Frame 2: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)

Ethernet II, Src: Zte_91:1c:b7 (74:a7:8e:91:1c:b7), Dst: Apple_be:f4:8c (f0:18:98:be:f4:8c)

Internet Protocol Version 4, Src: 192.168.2.254, Dst: 192.168.2.14

User Datagram Protocol, Src Port: 53, Dst Port: 52175

Domain Name System (response)

Transaction ID: 0x2c0d

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

twitter.com type A, class IN

Answers

twitter.com: type A, class IN, addr 104.244.42.129

twitter.com: type A, class IN, addr 104.244.42.1

[Request In: 1]

Time: 0.011071000 seconds

0000	f0 18 98 be f4 8c 74 a7 8e 91 1c b7 08 00 45 00t.....E..
0010	00 59 00 00 40 00 40 11 b4 37 c0 a8 02 fe c0 a8	..Y...@...7.....
0020	02 0e 00 35 cb cf 00 45 c9 2c 2c 0d 81 80 00 01	...5...E.,,.....
0030	00 02 00 00 00 00 07 74 77 69 74 74 65 72 03 63t witter.c
0040	6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 04	om.....
0050	ec 00 04 68 f4 2a 81 c0 0c 00 01 00 01 00 00 04	...h*... ..
0060	ec 00 04 68 f4 2a 01 22 21 cd 7a 66 02 c4 fe	...h*!"!zf...

DNS Encryption (2)

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

The image shows a Wireshark packet capture of a network session. The top pane displays a list of 16 packets. The bottom pane shows the details of the selected packet (No. 16), which is a DNS standard query response. The details pane is expanded to show the 'Domain Name System (response)' section, which includes transaction ID, flags, questions, answer RRs, authority RRs, additional RRs, and queries. The query is for 'twitter.com: type A, class IN'. The answers section shows the IP address 104.244.42.65. The bottom status bar indicates the frame is 147 bytes and the decrypted TLS is 63 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.017252	192.168.2.84	1.1.1.1	TLSv1.3	307	Client Hello
6	0.029492	1.1.1.1	192.168.2.84	TLSv1.3	195	Server Hello, Change Cipher Spec
8	0.030622	1.1.1.1	192.168.2.84	TLSv1.3	1522	Encrypted Extensions
9	0.030962	1.1.1.1	192.168.2.84	TLSv1.3	1246	Certificate, Certificate Verify, Finished
10	0.030965	1.1.1.1	192.168.2.84	TLSv1.3	279	New Session Ticket
13	0.195450	192.168.2.84	1.1.1.1	TLSv1.3	118	Change Cipher Spec, Finished
14	0.195451	192.168.2.84	1.1.1.1	DNS	107	Standard query 0x0000 A twitter.com
16	0.206893	1.1.1.1	192.168.2.84	DNS	147	Standard query response 0x0000 A twitter.com A 104.244.42.65 A 104.244.42.1

Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.2.84

Transmission Control Protocol, Src Port: 853, Dst Port: 54786, Seq: 3011, Ack: 371, Len: 85

Transport Layer Security

Domain Name System (response)

Length: 61

Transaction ID: 0x0000

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

twitter.com: type A, class IN

Answers

0000 00 3d 00 00 81 80 00 01 00 02 00 00 00 00 07 74 .-.....t

0010 77 69 74 74 65 72 03 63 6f 6d 00 00 01 00 01 c0 witter.c om.....

0020 0c 00 01 00 01 00 00 06 43 00 04 68 f4 2a 41 c0C..h.*A.

0030 0c 00 01 00 01 00 00 06 43 00 04 68 f4 2a 01C..h.*.

Frame (147 bytes) Decrypted TLS (63 bytes)

DNS Encryption (3)

●Mozilla Firefox

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

The screenshot shows the 'Connection Settings' dialog box in Firefox. The 'Use system proxy settings' option is selected. Below the proxy settings, the 'Automatic proxy configuration URL' field is empty. The 'No proxy for' field is highlighted with a blue border. Below this, the 'Example: .mozilla.org, .net.nz, 192.168.1.0/24' and 'Connections to localhost, 127.0.0.1, and ::1 are never proxied.' are shown. The 'Do not prompt for authentication if password is saved' and 'Proxy DNS when using SOCKS v5' options are unchecked. The 'Enable DNS over HTTPS' option is checked. The 'Use Provider' dropdown menu is open, showing 'Cloudflare (Default)', 'NextDNS', and 'Custom'. A tooltip for 'Custom' says 'Use the default URL for resolving DNS over HTTPS'. The 'Help' button is at the bottom left.

Connection Settings

☐ No proxy

☐ Auto-detect proxy settings for this network

☒ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy Port

☐ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port

FTP Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

☒ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

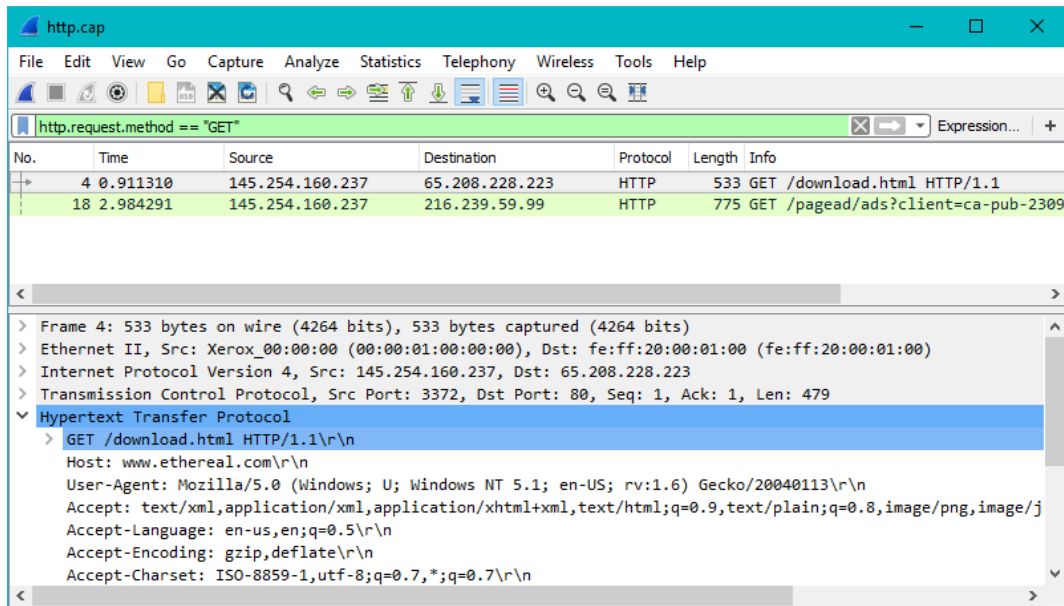
NextDNS

Custom Use the default URL for resolving DNS over HTTPS

Help

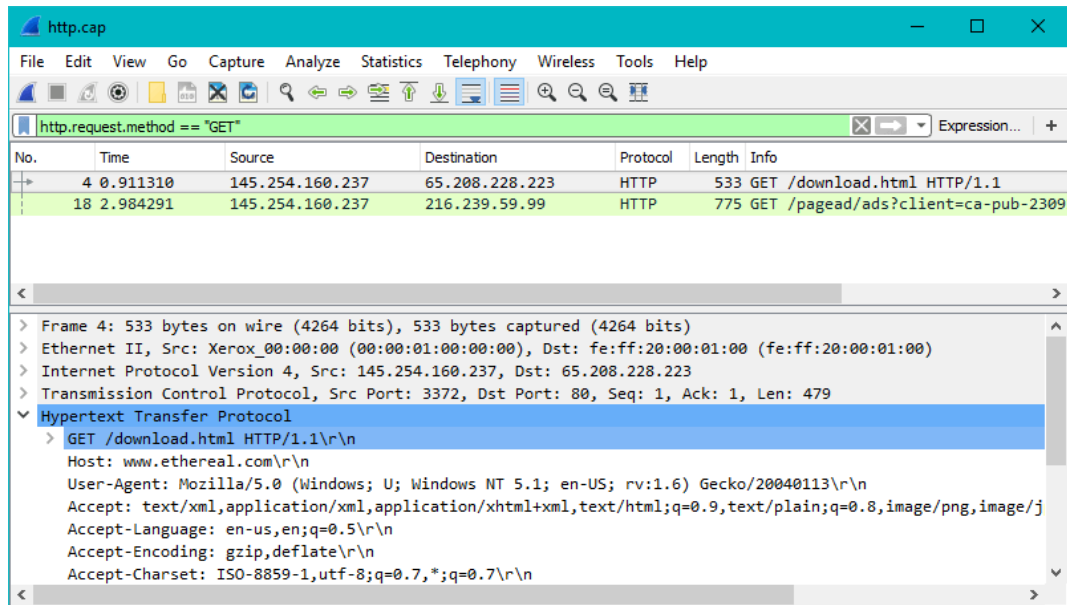
Http vs Https

- 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)

```
..ZZ.....#.....h2.http/1.1.....  
.....3.+.)zz..... m..  
+X..R...ONi..j,ZI"....S.r.Bs.-.....+..  
.....ZZ.....  
.....  
.....  
.....z...v...8.i....9.F.....Z .s3..e{n  
M..Ax...B.".....  
;Y..iD...X.%.....3,$... ..2cH. ...%,{...m,$..\...0.hg .  
+.....G.{F;c...g...6...dU.....{...  
0.n....t.=H.n.JoD.F.W.15.B..m.S=o]42VY...../....F.*..%]..1H..%MY.g.  
39.....X..\.....j...[...  
.....C.....7..(B...$..gu.....  
8.Y.k..F..t....m....MB...,...LbSf#...A.....G;Uk"# +.Q,...
```

Https vulnerabil?

- Aprilie 2014:

- In data de 7 aprilie 2014 a fost facuta publica o vulnerabilitate majora in OpenSSL, populara librerie 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)

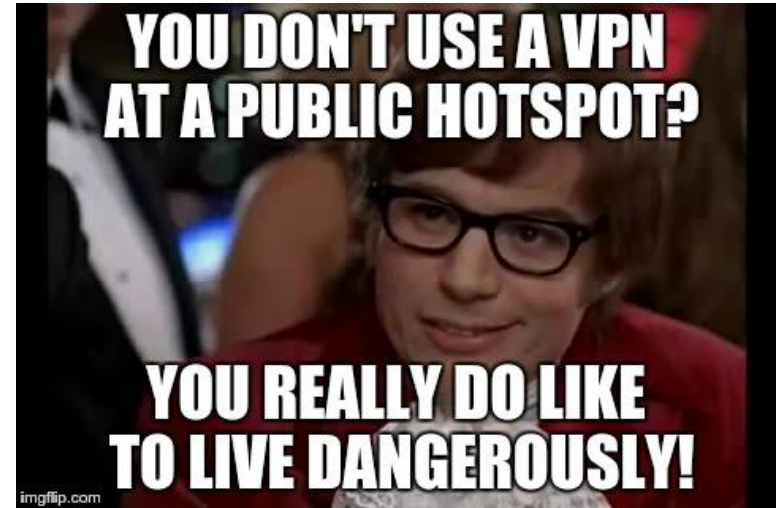


Server Key and Certificate #1

Subject	csm.ro Fingerprint SHA256: 56e822491f1e787e4c57ed503a5322df86645b536f83dfaaf7b31f0337ff83c Pin SHA256: w1xpEFUzSPXLB9ditLcBDwyZyzIVvRe5hcFEUcsal5U=
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 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**

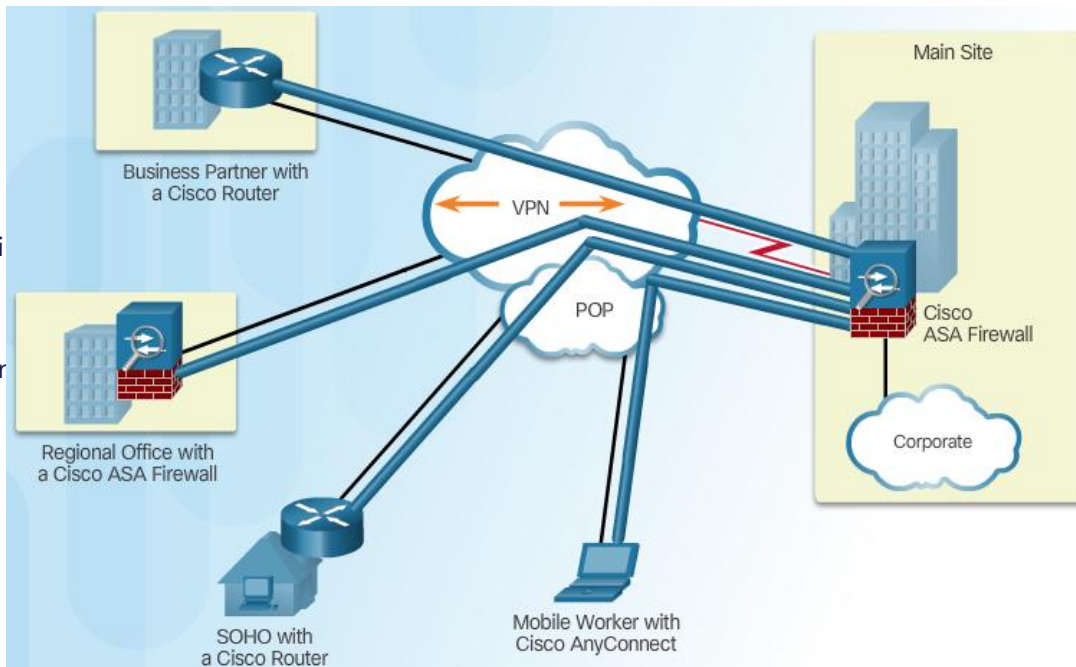
VPN-urile folosesc protocoale sigure de criptare și autentificare

- **Scalabilitate**

VPN-urile folosesc infrastructura existentă în Internet. 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 *IP/IP*

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

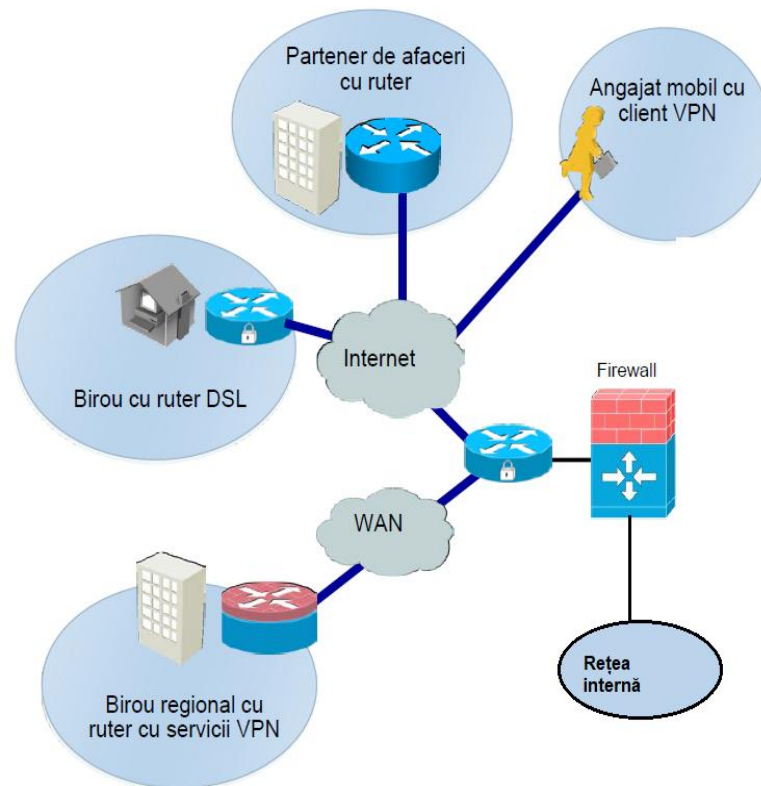


- *Antetul IP original nu este cunoscut rutelor intermediare!*

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

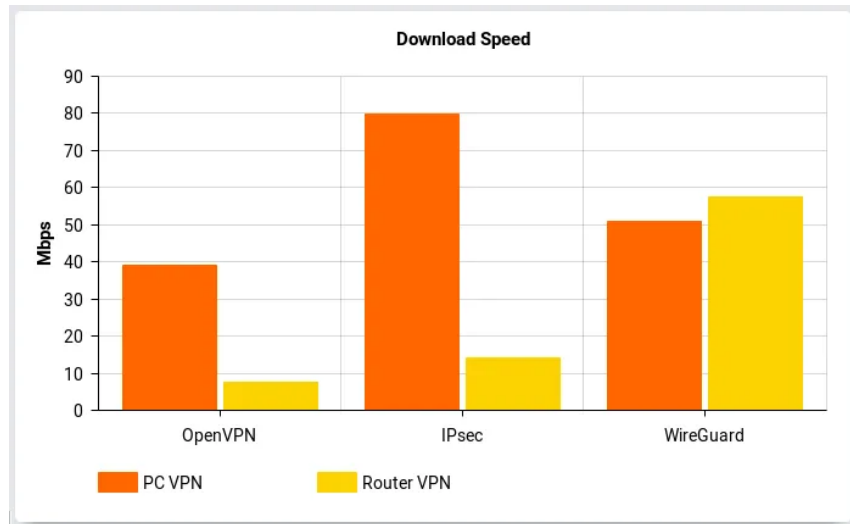
- Un VPN este un tunel care interconectează două puncte peste o rețea publică
- Pentru a transporta datele la destinație, un antet este adăugat la toate pachetele ce trec prin tunel (oferă toate beneficiile unui VPN)
- Antetul conține și informațiile de adresare ce permit pachetelor să ajungă la destinație
- 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:
```

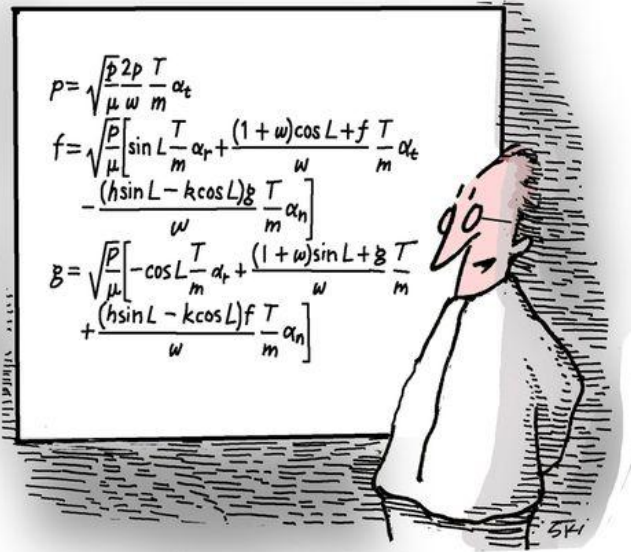
1	14 ms	9 ms	7 ms	192.168.23.1
2	19 ms	15 ms	9 ms	10.1.32.1
3	8 ms	15 ms	10 ms	node-bge.pool-1-2.dynamic.totinternet.net [1.2.185.254]
4	9 ms	9 ms	7 ms	172.20.241.5
5	10 ms	9 ms	13 ms	10.0.221.41
6	10 ms	9 ms	7 ms	10.0.200.178
7	8 ms	8 ms	8 ms	172.20.241.2
8	11 ms	8 ms	11 ms	10.255.10.1
9	9 ms	8 ms	8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



Any questions?

