PUNCT DE VEDERE TEHNIC

(Observatii la *Obiectiunile* DNA)

Expert tehnic:

CS I Prof. Univ. Dr. Ing. M. CARAMIHAI
FRI FAAPM MRSNZ MRSV MBCS MIEEE CIMP CRA

Expert desemnat:
VELCEA Marian
L.S.

CAPITOLUL I – PREZENTARE GENERALA

Prezentarea expertului
CS I Prof. Univ. Dr. Ing. Mihai CARAMIHAI, expert in domeniul automatica & informatica, aflat in evidenţa Biroului Central pentru Expertize Tehnice şi Contabile de pe lângă Ministerul de Justitie sub Nº 2807 – 8591

Obiectivul prezentului *Punct de vedere tehnic / raspuns la obiectiuni:*

Clarificarea unor aspecte existente in *Obiectiunile* formulate de catre DNA – Serviciul Teritorial Suceava, prin Serviciul Specialisti, in cadrul Dosarului Nº 1132/45/2011*, aflat pe rolul Tribunalului Suceava, Sectia Penala.

CAPITOLUL II – RASPUNSURI LA OBIECTIUNI

Elemente conceptuale : comunicatia prin email / autenticitatea email-urilor

Asa cum se poate vedea pe larg in *Anexa 1* prezentata la sfarsitul prezentului PVT, autenticitatea emailurilor (si *ipso facto*, certificarea inexistentei oricarei modificari a continutului acestora) este in general dificil de dovedit – acest lucru fiind posibil din punct de vedere tehnic numai in baza unor analize de detaliu.

*

* *

A. *Obiectiuni* formulate de catre DNA la *Raportul Expertului desemnat*

1. *Prima Obiectiune* formulata la *Obiectivul* expertizei are urmatorul continut « OB1. Concluziile raportului de expertiză nu răspund obiectivului dispus de instanţă.

Aşa cum s-a precizat prin încheierile de şedinţă din 26.09.2016 şi 24.10.2016 ale Tribunalului Suceava, obiectivul expertizei dispuse este de a stabili dacă e-mail- urile conţinute în cele 38 de fişiere indicate la filele 7 şi 8 din raportul de constatare tehnico-ştiinţifică din 04.04.2011 întocmit de specialistul DNA (filele 1-16 col. 13 dup), fişiere ce sunt imprimate pe suportul CD aflat la fila 17 voi. 13 dup, şi e-mail- urile indicate în procesele verbale de redare aflate la filele 21-97 din voi. 15 dup, filele 270-327 din voi. 40 dup, şi filele 371-381 din vol. 60 dup. (referite în continuare prin [e-mail-urile expertizei]) au suferit modificări atât cu privire la menţiunile privitoare la destinatar, expeditor, data transmiterii, cât şi cu privire la conţinutul e-mail-urilor.

OB1.01 Concluzia raportului de expertiză a fost formulată fără a se demonstra existenta măcar a unei singure modificări, fără a se preciza în ce constau modificările suferite de e-mail-uri, în ce condiţii au intervenit, cine anume le-a efectuat, ce mijloace tehnice au fost utilizate şi nici când anume s-au produs.»

Clarificare : Din punctul de vedere al subsemnatului, concluzia *Raportului de expertiza* s'a bazat pe urmatoarele argumente (specificate inclusiv in *Raport*) :

i. Tehnic: existenta unui acces extern la server, cf. *Raport*: „fişierul care conţine emailurile de expertizat (zzzz_ Vechi-2007) are data ultimei modificări ca fiind 14 septembrie 2010 orele 14:11 şi nu data ultimului mail transmis (22 octombrie 2009 Această constatare dovedeşte că pe data de 14 septembrie la orele 14:11 a avut loc ultima modificare a acestui fişier, fiind posibile şi alte modificări anterioare acestei date"

ii. Tehnic: inexistenta fisierelor de log aferente comunicatiei prin email, fapt ce poate fi luat in consideratie ca fiind un posibil rezultat al unei actiuni umane
iii. Logic: faptul ca exista *cu certitudine* o data de acces la server ulterioara datei de 16 Martie 2010, ora 17:33 nu exclude sub nici o forma (*modus ponens*) posibilitatea existentei unor accesari anterioare, cu efecte directe asupra veridicitatii datelor existente pe hardisk.

Raportul de expertiza nu si-a propus sa prezinte « existenta măcar a unei singure modificări, fără a se preciza în ce constau modificările suferite de e-mail-uri, în ce condiţii au intervenit, cine anume le-a efectuat, ce mijloace tehnice au fost utilizate şi nici când anume s-au produs» (toate aceste elemente nefiind solicitate prin *Obiectivul* dispus de *Instanta*) – ci doar sa prezinte elementele tehnice / logice in baza carora a fost formulata *Concluzia Raportului de expertiza.*

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

2. *A doua Obiectiune* formulata la *Obiectivul* expertizei are urmatorul continut « OB1.02 - în condiţiile descrise, concluzia raportului de expertiză se referă numai la unul dintre cele 38 de fişiere container, care împreună formează obiectul expertizei [e-mail-urile expertizei].»

Clarificare: Consideram ca aceasta *Obiectiune* este redundanta din punct de vedere logic : in cadrul Raportului a fost pusa in evidenta lipsa fisierelor *log* care sa marcheze trasabilitatea corespondentei email. *Ergo*, acest lucru este valabil pentru toate cele 38 de fisiere – container « care împreună formează obiectul expertizei [e-mail-urile expertizei].»

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

3. *A treia Obiectiune* formulata are urmatorul continut « OB2. Materialele digitale sursă (copiile efectuate la sediul DNA-S.T. laşi la 04.04.2017), pe baza cărora s-a efectuat analiza şi s-au formulat constatări şi concluzii în raportul de expertiză, nu sunt aceleaşi cu materialele digitale existente pe suporturile de stocare originale, componente ale sistemului HD01-Server de mail ALPIS»

Clarificare: Si in acest caz consideram ca Dl Expert face e eroare logica : acesta afirma ca nu poate « preciza motivele pentru care datele informatice existente la data 09 Noiembrie 2016 şi ora predării suporturilor D01 şi D02 către expertul desemnat nu coincid drept conţinut cu datele informatice existente pe aceleaşi suporturi D01 şi D02 la data 04 Aprilie 2017 » - in fapt fiind vorba d*e sume de control diferite* – si *nu* de continuturi diferite ale celor doua variante de clone. Sigur, in mod uzual, existenta unei identitati intre chei garanteaza identitatea de continut – dar reciproca nu este adevarata si asta pentru ca, pe de o parte, trebuie tinut cont de faptul ca algoritmul MD5 lucreaza cu octeti (bytes) si nu cu caractere si pe de alta parte, parametrul *timezone* era diferit in cazul celor doua proceduri / celor doi algoritmi (a se vedea in acest sens si Anexa 2).

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

4. *A patra Obiectiune* formulata are urmatorul continut « OB2.01 - Urmare valorilor diferite pentru cele două sigilii electronice (formate din sumele de control MD5 şi SHA1), s-a constatat cu

Expert tehnic consilier:
M. CARAMIHAI

certitudine faptul că datele informatice copiate la data de 04 Aprilie 2017 nu mai sunt aceleaşi cu datele informatice predate la 09 Noiembrie 2016.

Trebuie subliniat faptul că ambele operaţiuni de copiere au fost efectuate la sediul aceleiaşi instituţii şi cu acelaşi echipament de clonare/prelevare materiale digitale.»

Clarificare: Cf. *Clarificarilor* de la pct precedent, consideram ca, pentru cazul in care parametrul *timezone* a fost diferit in cazul celor doua operatii de clonare, este firesc ca si valorile cheilor de control sa fie diferite – fara ca acest lucru sa insemne ca *a fortiori* si continutul datelor este modificat.

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

5. *A cincea Obiectiune* formulata are urmatorul continut « OB2.02 - Din consultarea raportului de expertiză s-a constatat că datele informatice care au fost analizate în vederea îndeplinirii obiectivului sunt tocmai datele informatice copiate la data de 04 Aprilie 2017, iar formularea constatărilor şi concluziilor s-a bazat pe aceste copii.

Din practica judiciară a investigaţiilor digitale, în condiţiile în care sigiliul electronic al unei copii efectuate în condiţii legale este alterat, toate probele care au rezultat sau care pot rezulta din analizarea datelor informatice conţinute de aceste copii nu sunt admisibile în instanţă. »

Cf. *Clarificarilor* de la #4 si #5, nu a rezultat in nici un fel faptul ca avem un continut alterat al clonei 2 vs clona 1 (si este si greu de gasit o explicatie tehnica pentru o asemenea ipoteza – trebuind sa fie indicat in mod explicit „modificările suferite […], în ce condiţii au intervenit, cine anume le-a efectuat, ce mijloace tehnice au fost utilizate şi când anume s-au produs" cf. celor obiectate la #1 de Dl Expert.

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

6. *A sasea Obiectiune* formulata are urmatorul continut « OB2.03 Prin corelarea OB2.01 şi OB2.02, rezultă că toate constatările şi concluziile raportului de expertiză se bazează pe materialele digitale alterate, altele decât cele care au fost identificate şi localizate pe suporturile originale de stocare, componente ale sistemului HD0l-Server de mail ALPIS. Prin urmare, concluziile raportului de expertiză nu sunt admisibile.»

Clarificare: Asa cum s'a aratat la #4, #5 si #6, fiind vorba de niste premise false – este evident (modus ponens) ca si concluzia este falsa – drept pentru care consideram ca si *aceasta Obiectiune trebuie respinsa*.

7. In plus fata de aceste *Obiectiuni*, Dl Expert specialist I. Scriminti ofera si o analiza proprie a elementelor tehnice (i.e. « Analizarea datelor disponibile ») furnizand urmatoarele concluzii :
« E-mail-urile supuse expertizării, inclusiv e-mail-urile din fişierul container zzzzz_Vechi-20Q7 de pe HD01-Server mail ALPIS, au fost localizate şi identificate ca fiind înregistrate pe încă un alt suport de stocare, HD19-Hard- disk Seagate S/N : 9VPANXDW, localizat în stare latentă (neconectat la niciun sistem) şi ridicat la percheziţia domiciliară de la sediul unei persoane juridice.

Intrucât fişierul container de e-mail-uri identificat pe HD19-Hard-disk Seagate S/N : 9VPANXDW are data ultimei modificări 16.03.2010 orele 17:33, datorită identităţii absolute a e-mail-urilor conţinute de cele două fişiere zzzzz__Vechi-2007 localizate atât pe HD0l-Server mail ALPIS, cât şi pe HD19- Hard-disk Seagate S/N : 9VPANXDW, rezultă că e-mail-urile supuse expertizării

conţinute de aceste fişiere nu au suferit nicio modificare ulterior datei calendaristice de 16.03.2010 orele 17:33, respectiv :

- nici la data calendaristică 07 Aprilie 2010 (Anexa 3 pag. 38-30 Raportul de expertiză);
- nici la data calendaristică 12 Aprilie 2010 (Anexa 6 pag. 43-45
- Raportul de expertiză);
- nici în luna iunie 2010 (Anexa 4 pag. 40-41 Raportul de expertiză);
- nici la data calendaristică 14 Septembrie 2010 (Anexa 5 pag. 42 Raportul de expertiză);
- nici prin accesarea de două ori de pe calculatorul 3g- mihai2.bacau.rdsnet.ro în luna Septembrie 2010 (Anexa 7 pag. 46-47 Raportul de expertiză).

Toate materialele digitale prelevate în cadrul percheziţiilor informatice, inclusiv toate e-mail-urile supuse expertizei, sunt autentice şi sunt certificate prin sigiliile electronice formate din cele două sume de control MD5 şi SHA1, calculate, verificate şi consemnate în procesele verbale de percheziţie informatică, aflate la dosar. »

Clarificare: Consideram ca Dl Expert face o analiza ce excede *Obiectivelor* formulate de Tribunal, i.e. « să se stabilească dacă e-mail-urile supuse expertizei au suferit modificări atât cu privire la menţiunile privitoare la destinatar, expeditor, data transmiterii, cât şi cu privire la conţinutul e-mail-urilor. *Obiectul expertizei îl vor constitui e-mail-urile conţinute în cele 38 de fişiere indicate la filele 7 şi 8 din raportul de constatare tehnico-ştiinţifică din 04.04.2011 întocmit de specialistul DNA (filele 1-16 vol. 13 dup), fişiere ce sunt imprimate pe suportul CD aflat la fila 17 vol. 13 dup, şi e-mail-urile indicate în procesele verbale de redare aflate la filele 21-97 din vol. 15 dup, filele 270-327 din vol. 40 dup, şi filele 371-381 din vol. 60 dup.*[subl ns] » si inca : « Expertiza se va realiza pe serverul de e-mail Alpis ridicat de la martora Mărgineanu Sorina la data de 22.10.2010 ».

Astfel, introducerea unui HDD suplimentar in activitatea de analiza tehnica (i.e. HD19-Hard- disk Seagate S/N : 9VPANXDW, „ridicat la percheziţia domiciliară de la sediul unei persoane juridice") nu poate fi acceptata atata vreme cat acesta nu face obiectul expertizei tehnice dispuse de Tribunal.

In aceste conditii consideram ca *aceasta Obiectiune trebuie respinsa*.

Expert tehnic consilier:
M. CARAMIHAI

CAPITOLUL III – CONCLUZII GENERALE

Analiza critica facuta de catre subsemnatul unor aprecieri generale / metode utilizate de catre DNA / Serviciul specialisti, nu face decat sa sublinieze faptul ca Obiectiunile formulate nu s'au bazat pe demonstratii tehnice in raport cu care sa poata fi formulate concluzii logice, ci pe judecati generale, valabile in context non-tehnic si care nu se bazeaza pe rationamente logico – demonstrative.

In aceste conditii, consideram ca *Tribunalul* nu trebuie sa ia in considerare in textul *Obiectiunilor* formularile nejustificate de o demonstratie tehnica, urmand a le inlatura ca atare si trebuie sa tina cont doar de *relevanta, materialitatea, integralitatea si autenticitatea* probelor informatice analizate in comun de catre experti in cadrul *Raportului de expertiza tehnica* depus la *Dosarul* cauzei.

==========

CS I Prof. Univ. Dr. Ing. M. CARAMIHAI
FRI FAAPM FAAFM MRSNZ MRSV MBCS MIEEE CIPM CRA

Anexa 1

Aspecte conceptuale privind comunicatia prin email / autenticitatea email-urilor

Comunicatia electronica se refera la modalitatea prin care o persoana poate realiza un schimb de informatii prin intermediul unui sistem informatic, cu precadere o retea de sisteme informatice, cea mai intalnita forma de comunicatie folosind internetul fiind *posta electronica* sau *e-mail*, mesageria instant, retelele de socializare (care de asemenea dispun de un client de mesagerie instant), etc.

Arhitectura si functionarea postei electronice se bazeaza pe un mecanism de adrese ce apeleaza serviciul DNS (*domain name server*) pentru a preciza serverul si de informatii relevante local (pentru a preciza numele utilizatorului); astfel o adresa de e-mail contine 2 campuri separate prin simbolul @(at), acestea fiind numele utilizatorului si numele serverului unde trebuie sa ajunga mesajul.

Componenta care ofera preluarea mesajelor de la clientii de mail si livrarea lor la serverele destinatare este SMTP (*Simple Mail Transfer Protocol*).

Pentru preluarea mesajelor de pe serverul de email cele mai folosite protocoale sunt IMAP (*Internet Message Acces Protocol*) si POP3 (*Post Office Protocol v.3*). Deosebirea cea mai importanta intre aceste doua protocoale este faptul ca IMAP permite descarcarea mesajelor doar la vizualizarea lor si descarcarea partiala a acestora. POP3 ofera o alta abordare, datand din vremea in care serverele si retelele dispuneau de o conexiune cu lungime de banda foarte mica: utilizatorul care a primit un mail il descarca in memoria interna a sistemului informatic si apoi mesajul era sters din server pentru a elibera memoria. Astfel IMAP ofera posibilitatea citirii postei electronice de pe mai multe device-uri, deoarece la citire acestea nu sunt sterse automat de pe server.

O exemplificare a modului in care mesajele e-mail sunt trimise si a modului in care componentele descrise mai sus interactioneaza este urmatorul scenariu: un utilizator cu adresa de email a@a.org doreste sa trimita un mesaj altui utilizator cu adresa de e-mail b@b.org, prin folosirea unui client de mail.

1) In momentul in care a va cere comanda de trimitere a mesajului clientul de e-mail va initia o conexiune SMTP catre serverul de mail local (*a.org*), pentru realizarea conexiunii fiind nevoie ca utilizatorul sa se autentifice cu numele de utilizator si parola (sau acesta le poate avea salvate local, iar clientul va realiza conexiunea)
2) clientul va cripta mesajul conform SMTP si il va trimite la serverul local *a.org*
3) serverul local *a.org* va determina pe baza e-mail-ului destinatie (*b.org*) serverul destinatie , va initia o cerere de obtinere a adresei serverului *b.org* (DNS) si apoi il va livra conform protocolului SMTP
4) serverul local *b.org* va transmite mesajul la destinatar prin intermediul protocolului SMTP.
5) pentru a accesa corespondenta, utilizatorul b, prin intermediul clientului de mail va folosi protocolul IMAP sau POP3

Expert tehnic consilier:
M. CARAMIHAI

Din punctul de vedere al securitatii postei electronice trebuie mentionat faptul ca de la momentul trimiterii mesajului de catre expeditor pana la ridicarea acestuia de catre destinatar, mesajul trebuie sa parcurga multe computere si servere intermediare pana sa ajunga la destinatie, fapt ce implica posibilitatea folosirii atacurilor de tip *Man-In-The-Middle* (MITM) pentru interceptarea sau citirea lor

De mentionat mai este de asemenea si faptul ca mesajele trimise prin serviciul de posta electronica nu sunt criptate i.e. in combinatie cu posibilitatea atacatorilor de a accesa mesajele prin diferite metode, se reduce drastic securitatea postei electronice, fiind bine-cunoscute imprejurarile in care IT-isti ale unor companii au functia explicita de a investiga si de a monitoriza posta electronica a altor angajati, din motive de securitate .

B. Aspecte tehnologice

Pentru a trimite un e-mail trebuie in prealabil sa fie cunoscuta adresa (electronica) a destinatarului, i.e. adresa de e-mail. In plus, este nevoie si de un program de transmitere de e-mail, d.e. *Mail sau Pine* (sub sistemul se operare Unix) sau *Internet Mail, MS Outlook Express, Eudora Pro* (sub sistemul de operare *Windows*), etc.

Un *mesaj de e-mail* este format din doua componente:

- *header* (antet) - este generat de programul de mail si contine informatiile necesare pentru ca mesajul sa ajunga la destinatie
- continutul mesajului - ceea ce se doreste transmis efectiv (la Inceput, sub forma unui sir de caractere, In prezent putand contine si elemente multimedia)

La randul sau, *headerul* este format din mai multe campuri specifice:

BCC: (blind carbon copy)	Copii trimise unei liste de cititori, la fel ca si copiile indigo (CC); linia de antet care listeaza destinatarii este stearsa automat din mesajul trimis: nici unul dintre destinatarii mesajului nu va sti cine a mai primit “copii blind”.
CC: (carbon copy)	Adresele la care se trimit copii ale mesajului.
Date :	Data la care a fost trimis mesajul (se completeaza automat de sistem)
Semnatura	Modalitate de adaugare a unor informatii suplimentare la mesajele trimise; sunt folosite pentru a include informatii suplimentare despre utilizator.
From :	Adresa de e-mail a expeditorului.
Message-ID :	Sir de identificare generat la trimiterea mesajului. Acest sir este unic pentru fiecare mesaj.
Organization :	Numele organizatiei propietare a calculatorului de pe care se trimiite mesajul.
Received :	Camp adaugat de fiecare calculator care primeste mesajul si Il trimite mai departe (calea de la expeditor la destinatar)
Reply-to :	Adresa la care expeditorul doreste sa primeasca raspunsul in cazul In care aceasta difera de cea de la care a fost trimis e-mail-ul.
Subject :	Descriere pe scurt a mesajului .
To :	Adresa de e-mail a destinatarului.

Singurul reper pe care il are sistemul de e-mail pentru a livra un mesaj il constituie adresa de e-mail a destinatarului. Aceasta este de forma: *nume_utilizator@adresa_server_mail,* unde:

- *nume_utilizator* este numele contului de mail pe care utilizatorul il detine (sau un *alias* definit pe masina acestuia).
- *adresa_server_mail* este o adresa IP.

Orice mesaj primit poate fi returnat expeditorului: el poate fi modificat sau i se pot anexa *attachement*-uri. Aceasta reprezinta operatia de *Reply*. Ea poate fi facuta in raport cu expeditorul (*Reply to sender*) sau In raport cu expeditorul Impreuna cu cei care au mai primit mesajul (*Reply to all recipients*). Mesajul poate fi trimis altor utilizatori care nu se afla In lista destinatarilor din mesajul original (*Forward*).

Mesajele pot fi salvate (organizate) in foldere, dupa cum urmeaza:

- Mesajele primite pot fi pastrate Intr-un folder specific *(inbox)*.
- Mesajele ce nu au fost trimise imediat pot fi salvate in *outbox*.
- Copia mesajului trimis destinatarului este salvata in folderul *sent-mail*.
- Mesajele nefinalizate pot fi pastrate In folderul *draft*.

Mesajele de e-mail contin numai caractere ASCII. Pentru a putea trimite si fisiere binare, ele trebuie codificate In fisiere ASCII. Cele mai folosite standarde de codificare / decodificare a fisierelor binare sunt

- *uuencode / uudecode*, pentru sistemele UNIX,
- *binhex*, pentru calculatoarele Macintosh
- *MIME* (*Multi-purpose Internet Mail Extensions*) pentru sistemele Windows.

Unele programe client de posta electronica pot oferi si alte tipuri de facilitati:

- *notificarea receptarii mesajului*: trimiterea automata a unui mesaj catre expeditor atunci cand mesajul trimis a fost salvat In *mailbox*-ul destinatarului;
- *notificarea citirii*: trimiterea automata a unui mesaj expeditorului atunci cand mesajul a fost citit de catre destinatar.

Erori
La trimiterea unui e-mail pot apare anumite erori care conduc la netransmiterea (blocarea) mesajului. Daca se intampla asa ceva, expeditorul va primi un mesaj ce va detalia cauzele eseculului:

Mesaj de eroare	**Cauza generarii mesajului de eroare**
Host unknown	adresa destinatarului este inexistenta
Unknown user	Destinatarul nu exista pe masina specificata.

Este posibil ca programul sa gaseasca si calculatorul destinatie si pe destinatarul mesajului, dar sa nu poata sa transmita mesajul din cauza erorilor din retea (nu este posibil contactul cu sistemul aflat la distanta; sistemul aflat la distanta este “mort” (din punct de vedere fizic) sau este gresit configurat).

Expert tehnic consilier:
M. CARAMIHAI

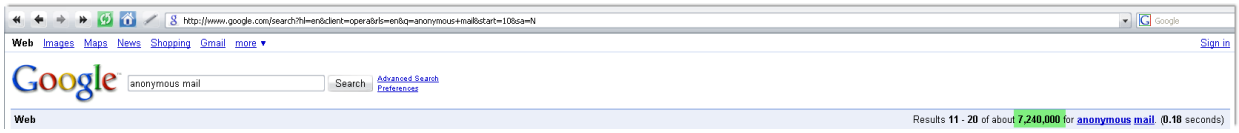
C. Emailuri false (Fake Emails): variante de lucru

In general, pe baza unei analiza critice conceptuale, mesajele de email nu pot fi in nici un caz considerate a fi cu certitudine *reale* (asa cum se va arata in cele ce urmeaza) din urmatoarele motive:

i. nu exista certitudinea ca mesajele au fost transmise intre adresele de email specificate
ii. nu exista certitudinea asupra faptului ca existenta contului emitator este datorata persoanei al carei nume figureaza in raport cu acesta (i.e. l'a creat, l'a utilizat, etc)
iii. nu exista certitudinea ca mesajele (si continutul acestora) nu au fost create de o terta persoana

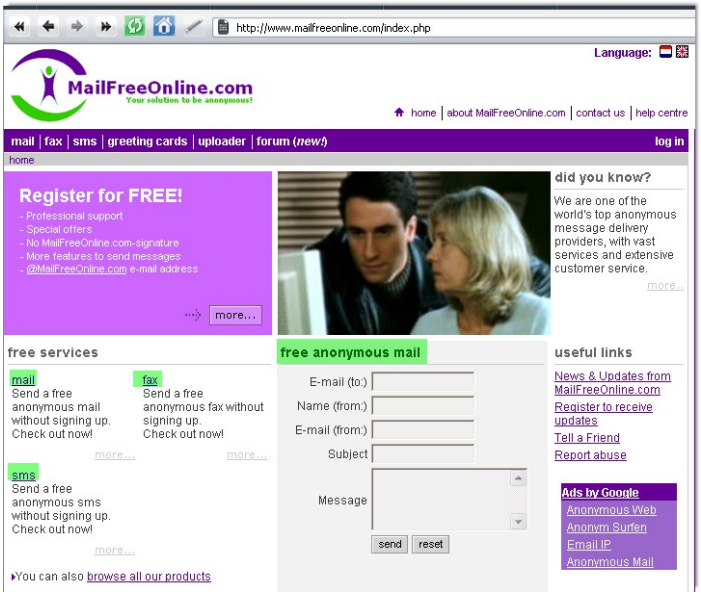
Aceasta analiza critica urmeaza a fi justificata in cele ce urmeaza.

Posibilitatea trimiterii de emailuri de la adrese fictive sau de la adrese reale, dar fara cunostinta proprietarului acestora, este posibila datorita diferitelor instrumente existente pe internet si a caror utilizare nu implica (in mod necesar) necesitatea unor cunostinte aprofundate in domeniul informatic. Cautarea pe *Google* a acestei optiuni ofera aprox. 7.200.000 (!) variante (cf. Figurii de mai jos)

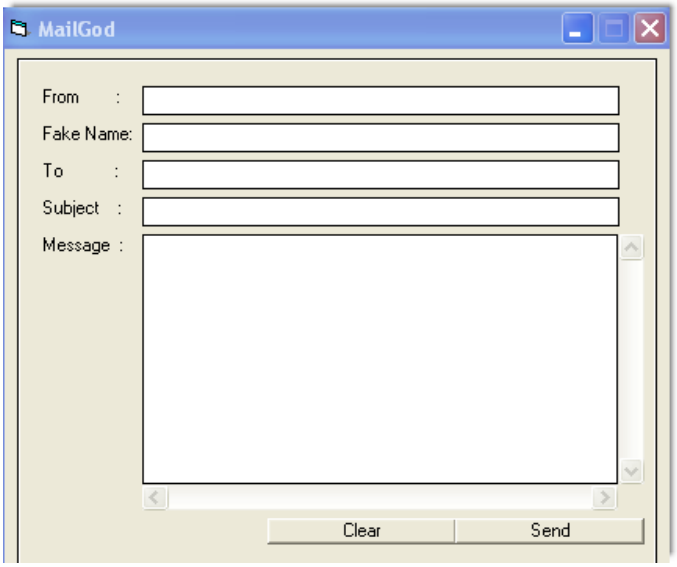


Astfel, unul din cele mai utilizate *site*-uri pentru trimiterea de mesaje email cu identitate falsa este https://www.anonymousspeech.com. Prin intermediul acestui *site* si prin crearea unui cont, orice persoana poate trimite un mesaj de la o adresa fictiva catre un destinatar real.

O alta varianta se gaseste la adresa http://www.mailfreeonline.com/index.php, adresa de la care pot fi trimise atat mailuri, cat si faxuri si sms-uri de la adrese fictive sau adrese reale, fara implicarea posesorului acestora. Se mentioneaza faptul ca asemenea transfer de informatie (cu mascarea emitatorului real) este posibil in afara unei expertize tehnice riguroase si in conditiile in care anumite informatii tehnice (v. mai sus) nu pot fi puse in evidenta de catre destinatarul mesajului:

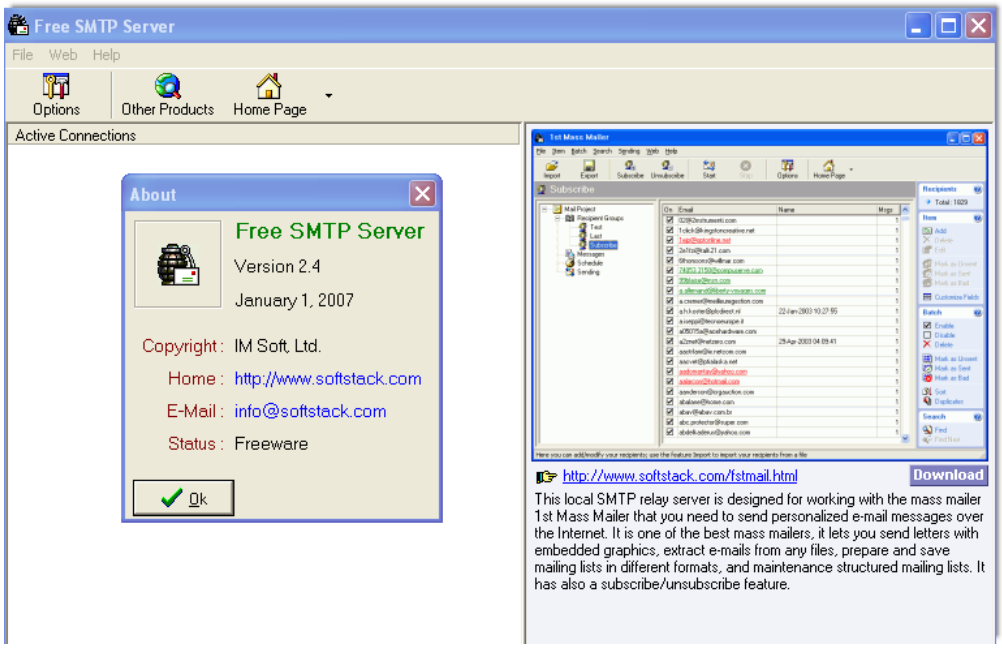


O metoda ceva mai profesionala, dar care implica anumite cunostinte tehnice de specialitate, presupune utilizarea unui program dedicat (d.e. *MailGod.exe*, descarcat de la adresa www.warez-god.org) si a carui interfata poate fi vazuta in figura de mai jos:



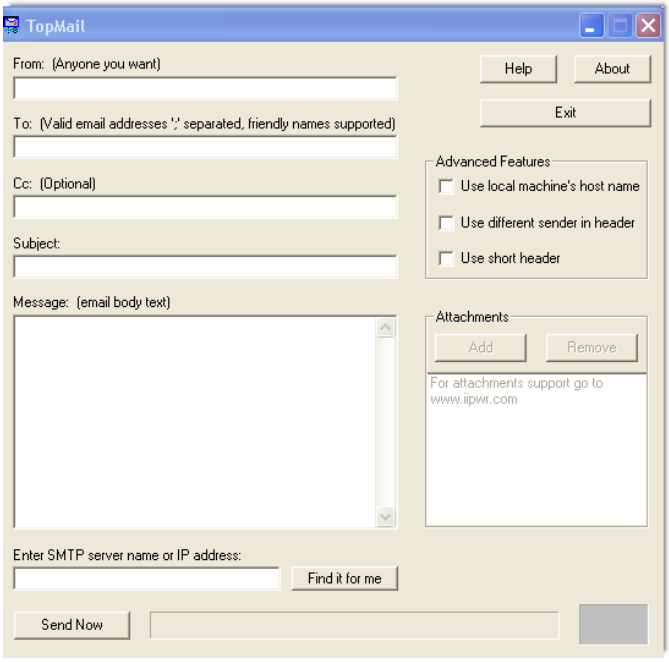
Programul trebuie utilizat (i.e. pentru a putea fi trimise emailuri anonime cuajutorul lui) in conjunctie cu un server SMTP, cum ar fi d.e. FreeSMTPServer descarcat de la adresa http://www.softstack.com/ :

Expert tehnic consilier:
M. CARAMIHAI



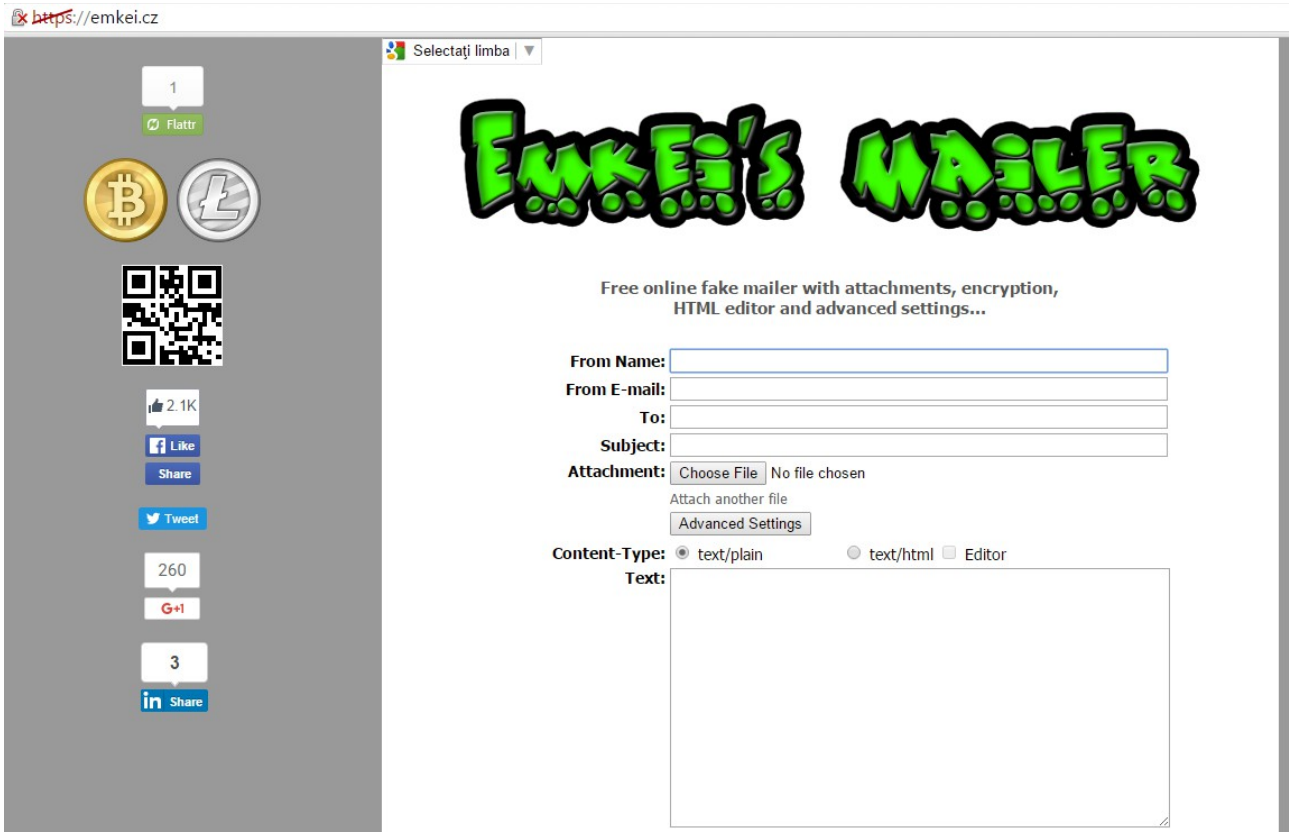
Astfel, serverul SMTP permite lansarea de pe calculatorul propriu a unor mailuri de la adrese oarecare (fictive sau reale), catre un destinatar precizat (si real)

In sfarsit, in raport cu acelasi concept de aplicatie aflata pe calculatorul propriu, poate fi utilizat un program mai simplu, si mai flexibil (care, in fapt, a fost folosit si in cadrul prezentei expertize) cum este *TopMail*, al firmei IIPwr, USA (**www.iipwr.com**):



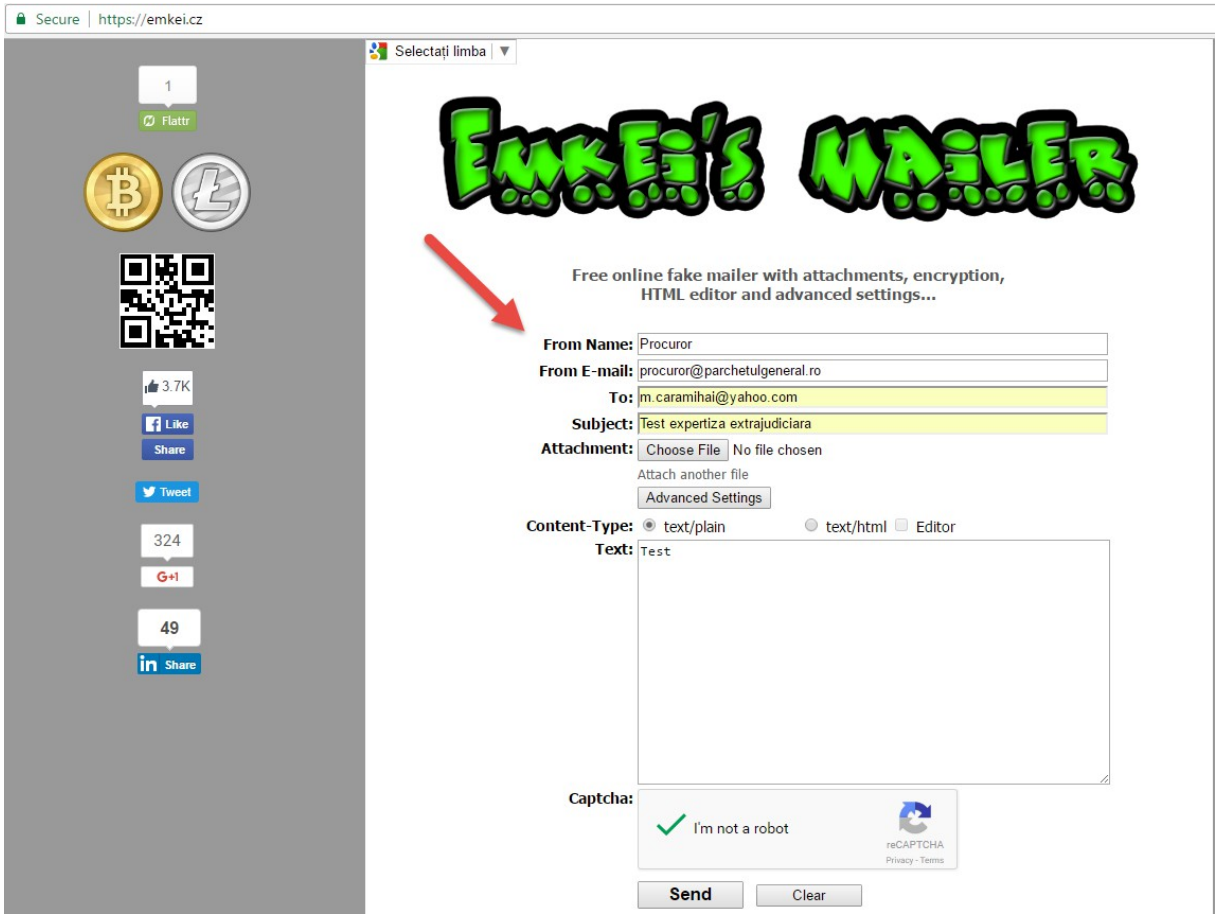
In sfarsit, o demonstratie simpla a non-validarii identitatii expeditorului in mediul virtual va fi facuta in cele ce urmeaza:

- se acceseaza o adresa de internet de undepoate fi trimis un email fals (*fake email*):



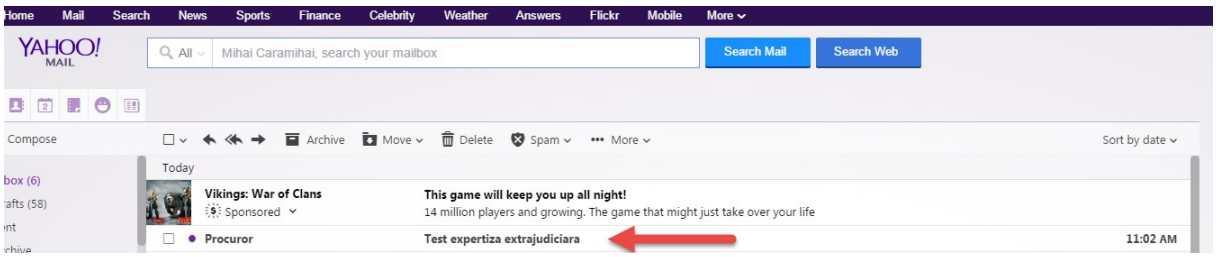
➲ se compune un mail fals, pe adresa expertului din partea *Procuror*, mail ce urmeaza a fi transmis expertului de la o adresa imaginara (i.e. procuror@parchetulgeneral.ro):

Expert tehnic consilier:
M. CARAMIHAI

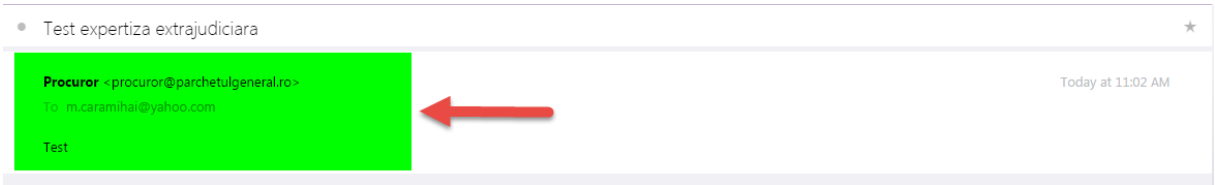


➲ transmiterea corecta a mailului

➲ se confirma ajungerea mailului la adresa de email a expertului, exact in forma in care a fost transmis, fara elemente de identificare suplimentara



adica



In aceste conditii, rezulta in mod nemijlocit faptul ca un mesaj (indiferent de continutul acestuia) poate fi transmis de la o adresa oarecare (reala sau nu) la o adresa reala prin intermediul unor operatii banale, ce nu necesita cunostinte informatice avansate. Evident, asemenea solutii pot fi dezvoltate individual, de catre un informatician cu experienta sau pot fi folosite si alte variante on-line, contra cost, ce ofera o anonimitate mai buna.

Expert tehnic consilier:
M. CARAMIHAI

Anexa 2

Functiile hash

Functiile *hash* (numite si *functii de dispersie* sau *functii de rezumat*; din EN: *hash functions*) reprezinta un algoritm matematic criptografic ce genereaza un *checksum* (rezumat criptografic) unic pentru fiecare mesaj. Acest *checksum* se numeste *Message Diggest, Diggest* sau *Hash*.

Functia hash *ideala* trebuie sa fie in mod simultan:

- *universala*: poti sa introduci orice parametru de intrare;
- *repetabila*: de fiecare data cand introduci variabila *X* vei obtine acelasi rezultat *Y*;
- *unidirectionala*: este usor sa calculezi valoarea functiei pe baza variabilei introduse in functie ($f(x) \rightarrow x$), dar imposibil sa afli variabila pe baza valorii functiei ($x \rightarrow f(x)$);
- *biunivoca*: ai garantia ca variabile diferite vor produce valori diferite ale functiei (*unicitate*) – dar si viceversa, ai garantia ca o valoare a functiei corespunde cu o singura variabila posibila;
- *concisa*: produce rezultate cu o marime predeterminata, indiferent de marimea variabilei de intrare.

Criteriul prioritar

Prima problema a functiei *hash* ideale o reprezinta o contradictie logica, ce nu poate fi rezolvata nici in lumea ideala a matematicii. Ne dorim ca functia *hash* sa fie in mod simultan *universala*, *biunivoca* si *concisa*. Or aceste trei cerinte nu se pot indeplini in mod simultan niciodata. Problema porneste de la cerinta *conciziei* — cu alte cuvinte, sa „incapa" intr-un numar oarecare de cifre. De exemplu orice numar natural mai mic de un milion incape intr-un spatiu de sase cifre. Asta cerem noi functiei hash *ideale*: vrem ca rezultatul ei sa incapa in N cifre. Evident, asta nu se poate daca ne mai dorim in plus ca functia sa fie in plus (1) biunivoca si (2) universala. Daca respectam (1) atunci putem accepta *cel mult* numere de N cifre (deci incalcam (2)); pe de alta parte, daca respectam (2) atunci va exista o infinitate de date de intrare pentru care vom produce aceeasi valoare de iesire (deci incalcam (1)).

Prin urmare nu se poate (nici macar teoretic) sa obtinem in mod simultan toate cerintele originale (biunivoca, concisa si universala). Pe de alta parte, stim conform definitiei ca avem nevoie de concizie (daca functia *hash* nu e concisa atunci marimea rezultatului creste cu valoarea de intrare).

Asadar, dintre cele trei caracteristici dezirabile (dar incompatibile), *concizia* este prioritatea cea mai importanta, i.e. trebuie sa cautam un compromis in jurul conciziei, sacrificand celelalte doua criterii ideale. Am ramas cu doua criterii intre care trebuie sa decidem prioritatea: biunivocitate si universalitatea. Asa cum se arata in literature de specialitate, ca universalitatea nu poate fi optionala: *trebuie* sa putem folosi functia *hash* pentru orice mesaj, parola sau fisier, indiferent de lungimea acestora. Asadar prioritatea criteriilor pentru o functie *hash* practica este urmatoarea:

1. concizie: marime constanta a rezultatului
2. universalitate: trebuie sa acceptam orice valoare de intrare
3. biunivocitate: doua valori de intrare diferite trebuie, pe cat posibil, sa produca rezultate diferite

Coliziuni

Prin „coliziune" se intelege situatia in care doua valori diferite de intrare produc aceeasi valoare de iesire a functiei *hash*. Cu alte cuvinte, coliziunile sunt situatiile in care se incalca biunivocitatea sumelor de control.

Algoritmi de *hashing*

1. MD5 - *Message Diggest Version 5*

- genereaza un hash pe 128 biti exprimat in 32 cifre hexazecimale;
- a fost creat de prof. Ronald Rivest de la MIT in 1991;
- a fost standardizat in RFC1321;
- este unul dintre cei mai folositi algoritmi de hashing in prezent (2009);
- incepand cu anul 2004 au inceput sa fie descoperite diferite vulnerabilitati in algoritm multe ne-fatale. Se considera ca va fi inlocuit in curand de alt algoritm mai sigur;

In exemplul de mai jos este pus in evidenta parametrul *timezone* (prin intermediul UTC) ce influenteaza marimea de iesire (https://www.w3.org/PICS/DSig/MD5_1_0.html):

```
The BNF below shows how a MD5 digest is encoded in a Resource Reference
Information Extension.

resinfo-data      ::= '(' HashAlgoURL resource-hash hash-date*1 ')'
HashAlgoURL       ::= '"http://www.w3.org/PICS/DSig/MD5_1_0.html"'
resource-hash     ::= '"base64-string encoding of 128 bit MD5 message
                        digest of the information resource."'
hash-date         ::= quoted-ISO-date
quoted-ISO-date   ::= '"'YYYY'.'MM'.'DD'T'hh':'mmStz'"'
     based on the ISO 8601:1988 date and time standard, restricted
     to the specific form described here:
     YYYY ::= four-digit year
     MM   ::= two-digit month (01=January, etc.)
     DD   ::= two-digit day of month (01 through 31)
     hh   ::= two digits of hour (00 through 23) (am/pm NOT allowed)
     mm   ::= two digits of minute (00 through 59)
     S    ::= sign of time zone offset from UTC ('+' or '-')
     tz   ::= four digit amount of offset from UTC
           (e.g., 1512 means 15 hours and 12 minutes)
     For example, "1994.11.05T08:15-0500" is a valid quoted-ISO-date
     denoting November 5, 1994, 8:15 am, US Eastern Standard Time
     Note: The ISO standard allows considerably greater
     flexibility than that described here.  PICS requires precisely
     the syntax described here -- neither the time nor the time zone may
     be omitted, none of the alternate formats are permitted, and
     the punctuation must be as specified here.
base64-string     ::= as defined in RFC-1521.
```

2. SHA1 - *Secure Hash Algorithm Version 1*

- genereaza un hash output pe 160 biti exprimat in 40 cifre hexazecimale;
- a fost creat si publicat de guvernul USA (NSA) in 1993;
- opereaza pe mesaje de maximum 2^64-1 biti;
- este unul dintre cei mai folositi algoritmi de hashing in prezent (2009);
- incepand cu anul 2004 au inceput sa fie descoperite diferite vulnerabilitati in algoritm multe ne-fatale. Se considera ca va fi inlocuit in curand de alt algoritm mai sigur;
- SHA2 este o noua familie de algoritmi de Hash publicati in 2001 care contine SHA-224, SHA-256, SHA-384 si SHA-512 dupa nr. de biti ai outputului;
- SHA3 reprezinta un nou protocol care este inca in dezvoltare si va fi supus unei competitii publice pana in 2012;

Expert tehnic consilier:
M. CARAMIHAI

In exemplul de mai jos este pus in evidenta parametrul *timezone* (prin intermediul UTC) ce influenteaza marimea de iesire (https://www.w3.org/PICS/DSig/SHA1_1_0.html):

```
The BNF below shows how a SHA1 digest is encoded in a Resource Reference
Information Extension.

resinfo-data      ::= '(' HashAlgoURL resource-hash hash-date*1 ')'
HashAlgoURL       ::= '"http://www.w3.org/PICS/DSig/SHA1_1_0.html"'
resource-hash     ::= '"base64-string encoding of 160 bit SHA1 message
                        digest of the information resource."'
hash-date         ::= quoted-ISO-date
quoted-ISO-date   ::= '"'YYYY'.'MM'.'DD'T'hh':'mmStz'"'
     based on the ISO 8601:1988 date and time standard, restricted
     to the specific form described here:
     YYYY ::= four-digit year
     MM   ::= two-digit month (01=January, etc.)
     DD   ::= two-digit day of month (01 through 31)
     hh   ::= two digits of hour (00 through 23) (am/pm NOT allowed)
     mm   ::= two digits of minute (00 through 59)
     S    ::= sign of time zone offset from UTC ('+' or '-')
     tz   ::= four digit amount of offset from UTC
           (e.g., 1512 means 15 hours and 12 minutes)
     For example, "1994.11.05T08:15-0500" is a valid quoted-ISO-date
     denoting November 5, 1994, 8:15 am, US Eastern Standard Time
     Note: The ISO standard allows considerably greater
     flexibility than that described here.  PICS requires precisely
     the syntax described here -- neither the time nor the time zone may
     be omitted, none of the alternate formats are permitted, and
     the punctuation must be as specified here.
base64-string     ::= as defined in RFC-1521.
```

3. Whirlpool
   - a fost creat in 1995;
   - produce un hash de 512 biti;
   - este o functie noua de hashing care poate opera cu mesaje de maxim de 2^256 biti;

4. Tiger
   - optimizat pentru procesoarele pe 64 biti;
   - outputul poate fi de 128 sau 160 pentru compatibilitate cu algoritmii mai vechi sau 192 biti;

Tipuri de atacuri asupra functiilor de hash
Asupra functiei hash se pot declansa diferite atacuri de tipul:

1. Collision attack
Presupune gasirea a doua mesaje oarecare cu acelasi hash in mai putin de 2^(L/2) iteratii. Acest tip de vulnerabilitate nu reprezinta o problema de securitate.

2. First pre-image attack
Presupune gasirea unui mesaj care determina un *hash* dat in mai putin de 2^L iteratii. Acest tip de vulnerabilitate reprezinta o grava problema de securitate.

3. Second pre-image attack
Presupune gasirea unui mesaj M2, avandu-se un mesaj M1 care sa determine acelasi hash in mai putin de 2^L iteratii. Acest tip de vulnerabilitate reprezinta o grava problema de securitate. L = lungimea hash-ului rezultat

Expert tehnic consilier:
M. CARAMIHAI