STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.8(88)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.144-147

PARTICULARITĂŢILE PROBLEMELOR CARE URMEAZĂ A FI SOLUŢIONATE ÎN CADRUL INVESTIGĂRII CRIMINALISTICE A INFRACŢIUNILOR INFORMATICE

Svetlana PURICI

Universitatea de Stat din Moldova

Scopul principal al acestui studiu nu este de a releva regulile generale ale admisibilităţii probelor (pentru că pornim de la supoziţia că acesta este un fapt cunoscut de cititori), ci reprezintă un studiu cu privire la problemele specifice ale „investigării criminalităţii cibernetice" în procesul penal şi criminalistică.

Cuvinte-cheie: *expert, expertiză, laborator, sistem de fişiere, suport de informaţii, program, format digital.*

PARTICULARITIES OF THE PROBLEMS TO BE SOLVED IN FORENSIC INVESTIGATION OF CYBERCRIME

The main task of this study is not to show the general rules of admissibility - because we are starting from the supposition that it's a known fact by the readers - but it will present a study about specific rules of the "cybercrime investigations" in the criminal procedure law and forensics.

Keywords: *expert, expertise, laboratory, file system, removable media, software, digital.*

Investigarea infracţiunilor informatice este o cerinţă ce se impune imperativ pe zi ce trece, în virtutea faptului că reprezintă o latură mai puţin studiată din perspectiva Procesului penal şi a ştiinţei Criminalistica.

Expertiza de bază şi cea mai importantă în cadrul investigării infracţiunilor informatice este cea a tehnicii de calcul şi a informaţiei stocate în ea ori, cum mai este numită în literatura de specialitate, tehnico-programistă sau tehnico-computerizată [1].

Efectuarea unei astfel de expertize la noi în ţară este posibilă în laboratorul de expertize judiciare inginero-tehnice de la Centrul Naţional de Expertize Judiciare sau cu atragerea specialiştilor cu calificarea respectivă din alte instituţii, chiar şi din alte state.

Pentru soluţionare, în faţa expertizei tehnico-programiste se pot acorda următoarele întrebări [3]:

1. Ce fel de informaţii conţin blocurile de sistem şi purtătorii magnetici? Care este destinaţia lor şi posibilităţile de utilizare?
2. Se conţin pe blocurile de sistem şi suporţi magnetici fişiere textuale? Dacă da, atunci care este conţinutul şi posibilităţile de utilizare a acestora?
3. Se află informaţie distrusă pe suporţii magnetici prezentaţi? Este posibilă restabilirea ei? Dacă da, atunci care este conţinutul şi care sunt posibilităţile de utilizare?
4. Ce fel de produse de program se conţin pe suporţii magnetici? Care este conţinutul lor, destinaţia şi posibilitatea de utilizare?
5. Putea oare blocul de sistem, prezentat spre cercetare, să fie scos intenţionat din funcţiune de către posesorul lui? Dacă da, atunci prin ce metodă? [2, p.77].
6. Se află pe suporţi magnetici programe specializate, utilizate pentru selectarea parolei sau a altui procedeu de pătrundere ilegală în reţeaua de calculatoare? Dacă da, atunci care sunt denumirea şi particularităţile lor, posibilităţile utilizării acestora pentru pătrundere în reţeaua computerizată concretă?
7. Care este cauza inaccesibilităţii către purtătorul magnetic de informaţie prezentat spre cercetare? [2, p.83].
8. Sunt careva semne ce confirmă utilizarea programului concret pentru pătrunderea ilegală în reţeaua computerizată menţionată? Dacă da, atunci care este structura cronologică a acţiunilor necesare pentru pornirea programului concret sau pentru efectuarea unei operaţiuni concrete?
9. Este posibil, lucrând în reţeaua computerizată concretă, de a efectua în produsele de program careva modificări ale f
10. işierelor. Dacă da, atunci care, în ce mod şi de la care calculator pot fi făcute schimbări analogice?
11. Există posibilitatea de a primi acces la informaţia confidenţială care se află în reţeaua indicată? În ce mod se efectuează un astfel de acces?

12. În ce mod are loc accesul ilegal în reţeaua computerizată locală? Care sunt semnele ce confirmă o astfel de pătrundere?
13. Dacă accesul ilegal la sistemul de operare a avut loc din afară, atunci care sunt posibilităţile de identificare a calculatorului de la care a avut loc accesul?
14. Dacă lipsesc semnele pătrunderii în reţeaua de calculatoare de la un utilizator exterior, atunci se poate de constatat de la care calculator este posibil a efectua operaţiuni asemănătoare?
15. Pot fi înaintate spre soluţionare şi întrebări privind compatibilitatea unor sau altor programe, posibilitatea utilizării programului concret la un calculator concret şi altele de acest gen?

În afară de acestea, putem acorda întrebări despre destinaţia unui sau altui obiect utilizat în tehnica de calcul, precum: care este destinaţia obiectului, care sunt posibilităţile utilizării şi ce fel de particularităţi constructive el are?; din ce părţi constă acesta?; a fost elaborat în condiţii industriale sau în condiţii artizanale?; dacă obiectul a fost confecţionat în condiţii artizanale, atunci în care sfere ale ştiinţei, tehnicii şi meşteşugăritului posedă cunoştinţe persoana care a creat acest obiect şi care este nivelul de pregătire a persoanei indicate?; poate fi compatibil obiectul menţionat cu alte obiecte, care sunt acestea?[*]

Întrebările soluţionate în cadrul Laboratorului examinări tehnologii informaţionale[**].

Întrebări de cercetare a hardului:

1. Aparţine dispozitivul prezentat la mijloacele computaţional-tehnice?
2. La care tip (marcă, model) se referă acest mijloc?
3. Care este destinaţia funcţională a acestui aparat?
4. Care este rolul şi care sunt posibilităţile funcţionale ale aparatului dat în sistemul computaţional concret?
5. Se referă acest aparat la sistemul computaţional prezentat?
6. Se foloseşte aparatul dat în soluţionarea unei sarcini funcţionale concrete?
7. Care a fost starea iniţială a aparatului (configuraţia, caracteristica)?
8. Care este starea reală a aparatului prezentat la cercetare (funcţionează, nu funcţionează)? Are el abateri de la parametrii tipici (normali) şi careva defecte fizice?
9. Ce regimuri de exploatare sunt stabilite (instalate) în aparatul dat?
10. Defectul acestui aparat este cauzat de anumite reguli de exploatare?
11. Se consideră aparatul prezentat ca purtător de informaţie?
12. Care este tipul purtătorului de informaţie?
13. Ce metodă de păstrare a datelor posedă purtătorul dat?
14. Este accesibil pentru citire acest purtător de informaţie?
15. Care sunt cauzele inaccesibilităţii către purtătorul de informaţie?

Întrebări de cercetare a programelor:

1. Care este caracteristica generală a programului prezentat, din ce componente (mijloace) este el alcătuit?
2. Ce denumire, tip, versiune, fel de prezentare (real, ascuns, îndepărtat) are acest program?
3. Care sunt rechizitele elaboratorului şi ale stăpânului programului dat?
4. Care este componenţa fişierelor corespunzătoare ale programului, care sunt parametrii lor (volumul, data creării, atributele)?
5. Care este destinaţia funcţională a programului?
6. Posedă purtătorii de informaţie programe pentru realizarea unei anumite sarcini funcţionale?
7. Se foloseşte acest program la soluţionarea unei anumite sarcini funcţionale?
8. Care este starea de-facto a programului, capacitatea lui de lucru în realizarea funcţiilor concrete?
9. Are acest program posibilităţi de protecţie împotriva accesului nesancţionat şi copierii?
10. În ce mod sunt organizate posibilităţile de protecţie a acestui program?
11. Ce mijloace instrumentale ale programului (limba de programare, bibliotecile standarde) au fost folosite la elaborarea programului prezentat?
12. Fişierele programului au fost supuse modificărilor? Cum s-a reflectat aceasta? (necesită model de comparaţie).

[*] Recomandări metodice privind metodologia de investigare a criminalităţii informaţionale şi a fraudelor prin Internet, 2007, Ordin al Procurorului General.

[**] din cadrul Direcţiei Investigare Infracţiuni Informatice a Ministerului Afacerilor Interne.

13. Modificările introduse în program sunt direcţionate spre înfruntarea protecţiei acestuia? Se atinge rezolvarea anumitor sarcini după introducerea schimbărilor în respectivul program?
14. În ce mod au fost făcute schimbările în acest program (intenţionat, prin intermediul unui alt program, al greşelilor mediului programului, al defectului acestuia)?
15. Sunt prezente în programul dat funcţii negative, în urma cărora are loc nimicirea, blocarea, modificarea sau copierea informaţiei.

Întrebări de cercetare a informaţiei (a datelor)

1. Care sunt caracteristicile amplasării (repartizării) logice a datelor pe purtătorul de informaţie?
2. Ce proprietăţi, caracteristici şi parametri (dimensiunile, timpul când a fost creat-schimbat, atributele etc.) posedă datele de pe purtătorul de informaţie? (Se concretizează care date, de ex.: baze de date, documente Word, Imagini etc.) [4].
3. Ce tip de informaţie (deschis, închis, şters, arhivat) se află pe purtător?
4. În ce mod este organizat accesul (liber, limitat ş.a.) către (la) datele de pe purtătorul de informaţie şi care sunt caracteristicile lor?
5. Ce proprietăţi, caracteristici posedă mijloacele evidenţiate de protecţie a datelor şi care sunt căile de învingere (înfruntare, străbatere) a lor?
6. Ce particularităţi (semne) de depăşire a protecţiei (sau încercări ale accesului nesancţionat) se află pe purtătorul de informaţie?
7. Care este conţinutul datelor protejate?
8. Ce necorespunderi ale prezentării tipice au loc pe datele evidenţiate (încălcarea integrităţii, necorespunderea formatului, includerea dăunătoare ş.a.)?
9. Ce date pentru soluţionarea unei anumite sarcini funcţionale se află pe purtătorul de informaţie?
10. Ce date cu fapte şi împrejurări ale unei cauze concrete se află pe purtătorul de informaţie?
11. Ce date despre proprietar (consumător) al sistemului computerizat (denumiri, parole, dreptul la acces ş.a.) se află pe purtătorul de informaţie?
12. Ce date de pe documentele (mostrele) prezentate la expertiză sunt şi sub ce aspect (întreg, fragmentar) ele se conţin pe purtătorul de informaţie?
13. Care este starea iniţială a datelor de pe purtător (sub ce aspect, care este conţinutul şi ce caracteristici, atribute posedau datele înainte de a fi şterse sau modificate)?
14. În ce mod şi în ce împrejurări au fost executate acţiunile (operaţiunile) (modificarea, copierea, ştergerea) anumitor date pe purtătorul de informaţie?
15. Ce mecanism (succesiunea acţiunilor) de soluţionare a unei sarcini concrete este reflectat în anumite date de pe purtătorul de informaţie?
16. Ce cronologie a succesiunii acţiunilor (operaţiunilor) cu datele evidenţiate a avut loc în procesul de soluţionare a unei sarcini concrete (de ex.: pregătirea imaginilor semnelor băneşti, a hârtiilor de valoare, imprimat al ştampilei etc.)?

Întrebări de cercetare complexă a sistemului computaţional
(în expertiza complexă a sistemului computaţional)

1. Reprezintă (este considerată) instalaţia prezentată un sistem computaţional?
2. Reprezintă instalaţia prezentată un întreg al sistemului computaţional sau este o parte a lui?
3. La ce tip (marca, model) se referă sistemul computerizat?
4. Ce componenţă (configuraţie) şi caracteristici tehnice posedă sistemul computaţional?
5. Este oare configuraţia sistemului computaţional tipică sau lărgită (extinsă) în soluţionarea sarcinilor concrete?
6. Pot fi soluţionate oare cu ajutorul sistemului computaţional prezentat anumite sarcini funcţionale (de consum)?
7. De ce purtători de informaţie dispune sistemul computaţional prezentat? Este realizat în sistemul computaţional careva sistem de protecţie a informaţiei?
8. Ce sistem de protecţie a informaţiei are sistemul computaţional prezentat? Care este modelul, tipul şi caracteristicile acestui sistem de protecţie?

Întrebări mai des întâlnite la îndeplinirea expertizelor

1. Se referă obiectul prezentat la mijlocul computaţional?

2. Reprezintă obiectul expertizei un sistem computaţional sau este o componentă a lui (aparat, program, informaţie)?
3. Care este tipul (marca, modelul), configuraţia şi caracteristicile tehnice generale ale sistemului computaţional dat (sau ale părţilor sale)?
4. Sunt soluţionate cu ajutorul sistemului computaţional prezentat anumite sarcini funcţionale (se indică care anume)?
5. Se află sistemul computaţional în stare de lucru? Au loc careva dereglări în activitatea lui?
6. Au loc careva încălcări ale regulilor de exploatare a sistemului computaţional (se indică caracteristicile programelor concrete care ne interesează)?
7. Este realizat (prezent) în sistemul computaţional un careva sistem de protecţie la accesul de informaţie? Care sunt posibilităţile de depăşire a lui?
8. Ce purtători de date posedă sistemul computaţional prezentat?
9. De ce tip (model, marcă) şi parametri dispune purtătorul de date prezentat?
10. Ce dispozitiv este destinat pentru lucrul cu purtătorul de date prezentat? Are sistemul computaţional prezentat dispozitiv destinat pentru lucrul (citirea, înregistrarea) cu purtătorul de date indicat?
11. Ce caracteristică generală şi destinare funcţională posedă programul obiectului prezentat?
12. Care sunt rechizitele elaboratorului, deţinătorului de drepturi al programului prezentat?
13. Sunt prezente pe purtătorii de date programe pentru soluţionarea unei sarcini concrete?
14. Care este destinaţia funcţională a programului aplicat prezentat?
15. Ce informaţie, care se referă la circumstanţele cauzei (se indică date concrete sau cuvinte-cheie), se conţine pe purtătorii de date? De ce tip este (deschis, închis, şters, arhivat)?
16. Conţine purtătorul de date informaţie autentică după conţinut cu modelele prezentate? De ce tip este (deschis, închis, şters, arhivat)?
17. Cărui format corespund datele evidenţiate (documente textuale, failuri grafice, baze de date ş.a.) şi cu ajutorul căror programe ele pot fi prelucrate?
18. Ce informaţie despre proprietar al sistemului computaţional (inclusiv nume, parole, drepturi la acces etc.) se conţine pe purtătorul de date?
19. Sunt prezente caracteristici privind accesarea reţelei Internet cu ajutorul mijlocului computaţional prezentat? (Ce site-uri au fost accesate de pe sistemul computaţional, care este perioada?)
20. Sunt pe purtătorii sistemului computaţional programe soft pentru schimb rapid de mesaje (Skype, ICQ, Mirinda, TheBat. etc.)? Dacă da, afişaţi lista contactelor şi anexaţi conţinutul mesajelor din acestea pe un purtător de informaţie.

Sisteme de calitate în criminalistică[*]: În prezent, în cadrul Ministerului Afacerilor Interne a fost instituit un laborator criminalistic specializat, iar pentru acceptarea rezultatelor laboratorului în Moldova sau în comunitatea internaţională este critică implementarea celor mai performante practici în criminalistică şi elaborarea unui sistem de management al calităţii, similar celui aplicat de laboratoare pe plan internaţional (ISO 17025 şi ILAC G-19:2002). Pentru a corespunde standardelor internaţionale, experţii din cadrul laboratorului aplică metodologii testate şi validate ce pot fi repetate şi verificate/măsurate. Aceste proceduri sunt documentate (Proceduri Operaţionale Standard – SOPs) ca parte a sistemului de management al calităţii din cadrul laboratorului; de asemenea, acestea sunt respectate de experţi ca fiind fundamentul fiecărei examinări criminalistice a datelor în format digital.

Bibliografie:

1. DOBRINOIU, M. Provocarea legislativă a reţelelor WI-FI. În: *Revista Intelligence* (Bucureşti), 2009, nr.16, p.56.
2. GHEORGHITA, M., BREGA, Z., VOZNIUC, L. şi al. *Ghid de expertize judiciare*. Chişinău: Î.I. „Angela Levinţa", 2005, p.77-83.
3. ЯРОЧКИН, В.Я. *Информационная безопасность: Учебник для вузов.* Москва: Gaudeamus, 2004, с.455.
4. КАНДЕРС, У. Возможные решения в борьбе против киберпреступлений в современных условиях. В: *Закон и Жизнь*, 2008, №4, с.23.

Prezentat la 23.04.2015

[*] Ministerul Afacerilor Interne. Conceptul de operaţiuni în dezvoltarea capacităţilor de investigare a delictelor cibernetice, crearea laboratorului criminalistic de expertiză a datelor în format digital, 2009.