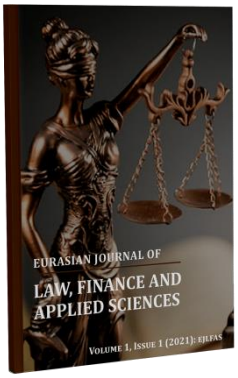
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 7.984 www.in-academy.uz



RAQAMLI TERGOV AMALIYOTIGA QARSHI VOSITALAR (ANTI-KRIMINALISTIKA)NING ILMIY-NAZARIY MASALALARI

Bobur Karimov
O'qituvchi, Toshkent davlat yuridik universiteti
Toshkent, O'zbekiston
b.karimov@tsul.uz
https://doi.org/10.5281/zenodo.10695404

ARTICLE INFO

Received: 16th February 2024
Accepted: 22th February 2024
Online: 23th February 2024

KEYWORDS

Anti-kriminalistika, tergovga qarshi vositalar, buzuvchi texnologiyalar, raqamli kontent, o'chirish, ma'lumotlarni zararlash, anti-kriminalistika izlari.

ABSTRACT

Ushbu maqolada raqamli tergov amaliyotiga qarshi qo'llaniladigan anti-kriminalistik vositalar tushunchasining ilmiy va nazariy tavsifi tahlil qilingan. Bunda anti-kriminalistik vositalarning ma'lum potensial dalillarga yetkazishi mumkin zararlar, ularning qo'llanish maqsadlari va usullariga ko'ra tavsiflash masalalari ko'rib chiqilgan. Shuningdek, ushbu maqola raqamli kriminalistika amaliyotchisining raqamli ma'lumotlarni to'g'ri tiklash va sharhlash qobiliyatini buzishi mumkin bo'lgan jarayonlarga e'tibor berish zarur bo'lgan, mutaxassisni chalg'ituvchi jihatlari bayon qilingan.

Raqamli ma'lumotlar shakllari jinoyatlarni tergov qilish va ta'qib qilishda muhim rol o'ynaydi. Bugungi kunda raqmli dalillarni tekshirish samaradorligiga to'sqinlik qilishiga qaratilgan vosita va usullar ortib bormoqda. Ushbu vositalar ilk bor 2009-yilda Pajek va Pimenidislar tomonidan e'tirof etilgan. Ushbu tadqiqotchilar bunday qarshi choralar ko'rilgan holda tergov o'tkazish juda qimmat yoki ko'p vaqt talab qiladi, deb hisoblaydi. Bunday vaziyatlarda odatda, ish tashlab ketilishi mumkin, tergovchilar esa mag'lubiyat hissi bilan qoladilar [1]".

Kriminalistik nuqtayi nazaridan ushbu vositalardan noqonuniy faoliyatni amalga oshirishda texnik ustunlikka erishish maqsadida foydalaniladi. Ushbu vositalar ham o'zidan iz qoldiradi. Masalan, biror mulkka kirish uchun buzish qurollaridan foydalanish kabi. Raqamli dalillarni bilan ishlash amaliyotida ham antikriminalistik vositalardan keng foydalaniladi.

Raqamli kriminalistika vositalarini ikkita katta guurhga ajratish mumkin. Bular: raqamli dalillar tadqiqoti uchun mo'ljallangan raqamli kriminalistik vostilar va antikriminalistik vositlar.

Raqamli kriminalistik vositalar doimiy xotiradagi ma'lumotlar bilan ishlash uchun mo'ljallangan (Sleuth Kit [2]) va vaqtinchalik xotiradagi (RAM, Kesh, Registr) o'zgaruvchan ma'lumotlarni tahlil qilishda qo'llaniladigan vositalaridan (NetIntercept [3]) iborat [4].

"Anti-kriminalistika" (AK) vositalari tergovga qarshilik ko'rsatish va kibermakonda sodir etilgan jinoyatlar izlarini yashirish uchun mo'ljalangan vositalardir.

Lyu va Braun anti-kriminalistika vositalardan foydalanishning quyidagi maqsadlarini ko‘rsatishgan [5]:

- hodisa sodir bo‘lganligini aniqlashga to‘sqinlik qilish;
- axborot to‘plash jarayoniga halaqit berish;
- ish bo‘yicha sarflashi kerak bo‘lgan vaqtni oshirish;
- ekspertiza xulosasi yoki ekspert ko‘rsatuvlariga shubha uyg‘otish.

Biroq bu yerda boshqa maqsadlar ham mavjud, masalan:

- raqamli kriminalistik vositalardagi bo‘shliqlar va zaifliklarni oshkor qilish;
- kriminalistika vositasini buzish yoki boshqa maqsadga o‘zgartirish;
- mutaxassisning o‘ziga to‘g‘ridan-to‘g‘ri hujum qilish (masalan, mutaxasisning tarmog‘ini aniqlash va masofadan o‘chirish yoki ekspert ishlayotgan bino serveriga hujum qilish);
- anti-kriminalistika vositasi ishga tushirilganligi haqida hech qanday dalil qoldirmaslik.

Anti-kriminalistik vositalariga qiziqish yildan-yilga ortib bormoqda. Ushbu vositalarni Darknet tarmog‘idan bepul olish mumkin. Ba’zi ishlab mutaxassislarning fikricha, ushbu vositalar mavjud kriminalistik vositalari va jarayonlarini yaxshilashga majbur qiladi. Shuningdek, bugungi kundagi raqamli kriminalistika vositalarning imkoniyatlarini ko‘rsatadi. Misol uchun, EnCase [6] kabi “ishonchlilik kafolati” deb tan olingan raqamli kriminalistik vositaga ham bugungi kunda xakerlar tomonidan buzib kirilgan. Ushbu holat dasturiy ta’minot orqali olingan natijalardan sudda dalil sifatida foydalanish imkoniyatini cheklab qo‘yadi. Boisi, ushbu vositalar “aybdor tomonni oqlashi” yoki “ma’lumotlarni joylashtirish orqali aybsiz tomonni ayblashi” mumkin.

Jinoyat izlarini tekshirishga salbiy ta’sir qiluvchi vositalar tergovni olib borish vakolatiga ega bo‘lgan subyetklarda ham (huquqni muhofaza qiluvchi organlar) xavotir uyg‘otadi. Ammo, tergov jarayonida bunday vositlardan foydalanish darajasi nisbatan noma’lumligicha qolmoqda.

Tergovga qarshi vositalar bo‘yicha raqamli kriminalistika sohasida olib borilayotgan emperik tadqiqotlar juda kam. Mavjudlari ham nazariy jihatdan tahlil etilgan, biroq amaliy xarakterga ega emas.

2016-yilda Konlan, Baggili va Breitinger [7] raqamli kriminalistika jarayonlariga to‘sqinlik qiluvchi tahdidlarni tekshirish va baholashga alohida ahamiyat qaratish (kuch, mablag‘) zarur, degan fikrni ilgari suradi. Bunday fikrni 2013-yilda Al Fahdi va boshqalar [8] tomonidan ham taklif qilgan. Ularning fikricha, tergov jarayonida tekshirilayotgan qurilmani to‘liq tushuna olmaslik, jinoyat izlarini aniqlash va boshqa bir qator isbot qilish bilan bog‘liq texnik muammolar yuzaga keladi.

Anti-kriminalistika tushunchasi raqamli kriminalistikada qabul qilingan bo‘lib, standart qurilmani topishi yoki raqamli dalillarning ishonchliligini shubha ostida qoldirish bilan bog‘liq jarayonlarni tavsiflash uchun ishlatiladi.

Anti-kriminalistika vositalaridan operatsion tizimlar va qurilmalarni “buzuvchi texnologiyalar” sifatida foydalanish raqamli kriminalistika jarayonlariga salbiy ta’sir ko‘rsatishi mumkin. Anti-kriminalistika atamasi bilan bog‘liq muammo shundaki, uni istalgan vaqtda raqamli tergov jarayonlariga to‘sqinlik qiladigan barcha dasturiy ta’minot va apparat vositalarini o‘zboshimchalik bilan tasniflash uchun qo‘llash mumkin.

Anti-kriminalistik vositalardan maxfiylikni kuchaytiruvchi dasturiy ta’minot sifatida foydalanish mumkin. Masalan, tizimda Internet faoliyati tarixini kamaytirishi mumkin [9].

Anti-kriminalistika ta’rifi bilan bog‘liq masalalar Al Fahdi [10] tomonidan olib borilgan tadqiqotlarda ham yoritilgan. Muallif anti-kriminalistik vositalarning bir shakli sifatida shifrlash va steganografiyaga e’tibor qaratgan. Har ikki usul ham anti-kriminalistika jarayonining bir qismini tashkil qilishiga qaramasdan, ular har doim ham anti-kriminalistik vosita hisoblanmaydi. Ushbu usullar maxfiylik va xavfsizlikni kuchaytirish maqsadida ham qo‘llanilishi mumkin.

Anti-kriminalistik vositalar ta’rifini ishlab chiqishda uni qanday maqsadda foydalanilganligiga e’tibor qaratish maqsadga muvofiq. Mantiqan, “anti – qarshi, teskari” biror narsaga qarshi degan ma’noda qo‘llaniladi, kriminalistika atamasi esa “jinoyatni o‘rganish haqidagi fan” sifatida nazariyaga kiritilgan. Demak, anti-kriminalistik deb topish uchun vosita kriminalistik tadqiqotlarga to‘sqinlik qilishi zarur [11].

Anti-kriminalistik vosita atamasi kontseptual jihatdan yangi bo‘lmasa-da, nazariyada uning ta’rifi hali o‘z isbotini topgani yo‘q (Harris, 2006). Rojers (2006) anti-kriminalistik vositalarga “jinoyat joyidagi dalillarning mavjudligi, miqdori va / yoki sifatiga salbiy ta‘sir ko‘rsatuvchi yoki dalillarni tekshirishni qiyin yoki imkonsiz qilishga qaratilgan vositalar” deb ta‘rif bergan. Liu va Braun (2006), anti-kriminalistika sud tekshiruvi uchun faktik ma‘lumotlarni bekor qilish maqsadida raqamli tadqiqotlarga nisbatan ilmiy usullarni qo‘llash, deb ta’riflagan [12].

Anti-kriminalistik vositalar tergov jarayonida to‘plangan dalillarni buzish uchunmi yoki kompyuter tizimini yaxshilashga urinish uchunmi tergov jarayonida [13] bunga aniqlik kiritilishi lozim.

Anti-kriminalistika tushunchasi raqamli kontentni olish va talqin qilish jarayonini buzishi mumkin bo‘lgan harakatlarning qamrab oladi. Tergov jarayoniga xalaqit berish qasd qilinishi kerak. Muammo shundaki, agar foydalanuvchining dastlabki maqsadi tizim ish faoliyatini yaxshilash bo‘lsa va bunday jarayonlar natijasida raqamli tekshiruv davomida foydali bo‘lishi mumkin bo‘lgan ma’lumotlar buzilgan bo‘lsa, bunday harakatlar anti-kriminalistik vosita bo‘lishi mumkin emas. Anti-kriminalistika uchun mo‘ljallanmagan vosita anti-kriminalistik vosita bo‘la olmaydi. Biroq, bunday jarayonlar anti-kriminalistika rejimida ishlatilishi mumkin, masalan, “disk-defrag” kabi standart protseduralar fayllarni tiklash potensialini kamaytiradi, shuningdek, qonuniy ishlash qobiliyatini oshirish uchun mo‘ljallangan bo‘lishi mumkin.

Anti-kriminalilstik vosita deb baholash fikr va tafakkur mahsulidir. Ehtimol, anti-kriminalistika bu atama bo‘lib, u faqat kriminalistik jarayonlarga qarshi kurashish maqsadidagi tor ilovalar to‘plamiga nisbatan qo‘llanilishi mumkin. Bunday vositalar jinoyatchini javobgarlik va jazodan qutilib qolishi uchun uchun ishlab chiqilgan bo‘lishi shart.

Biroq, bu vositalar raqamli kriminalistika sohasida yuzaga keladigan xavflarni to‘liq aks ettirmaydi. Raqamli kriminalistika jarayonlarini buzish sohasiga nisbatan quyidagi ikki xavf toifasi mavjud:

1-toifa: maxsus anti-kriminalistik vositalari;

2-toifa: buzg‘unchi texnologiyalar.

Mavjud raqamli dalillarni niqoblash yoki o‘chirish uchun ishlatilishi mumkin bo‘lgan juda ko‘p anti-kriminalistik vositalari mavjud. Raqamli kriminalistika sohasi tahdidni maxsus anti-kriminalistik vositalari (1-toifa) va passiv buzg‘unchi texnologiyalar (2-toifa) ning har ikkisi ham xavf tug‘dirishini tan olishi kerak.

1-Toifa: Maxsus anti-kriminalistik vositalari quyidagi oltita shaklda tasniflash mumkin. Masalan, ma’lumotlarni yashirish, o‘chirish, zararlash (shifrlash, siqish), o‘zgartirish (manipulyatsiya) qilish, tahrirlash, niqoblash, chalkashtirish [14], yo‘q qilish.

2-Toifa: “Buzg‘unchi texnologiyalar” qonuniy funksiya va maqsadga ega bo‘lib, ular tekshiruv jarayonlarida qurilmadagi ma’lumotlarga zarar yetkazishi mumkin. Ushbu turdagi har qanday vosita tergovga qarshi ishlatilishi mumkin.

Buzg‘unchi texnologiyalardan foydalanish bilan bog‘liq muammolarni ikki turga ajratish mumkin: birinchisi, muayyan buzg‘unchi texnologiyadan foydalanilganligini aniqlash – ularning funksiyasi qonuniy tizim faoliyati bo‘lib, ba’zi hollarda foydalanuvchining odatiy xatti-harakatlaridan farqlash qiyin;

Ikkinchisi, buzg‘unchi texnologiyadan anti-kriminalistik maqsadlarda foydalanilganligini aniqlash – ulardan foydalanishni maxfiylikni kuchaytiruvchi harakatlar kabi holatlardan farqlash zarur.

Birinchisi holatda zararli texnologiyalardan foydalanishni aniqlash ko‘p hollarda muammoli hisobalanadi. Ehtimol, bunday harakatlarni farqlashning hech qanday usuli yo‘q va bu vijdonli foydalanuvchini xavf ostiga qo‘yishi mumkin. Bunday aktlar raqamli kriminalistika sohasida anti-kriminalistikani aniqlashdagi qiyinchiliklarni yuzaga keltiradi. Natijada, barcha holatlarda sababni aniqlashning iloji bo‘lmasligi mumkin. Ammo, har qanday holatda ham ushbu texnologiyadan foydalanganlik holatini aniqlash muayyan tizimda dalillarning yo‘qligini tushuntirishga yoki ishonchliligini baholashga yordam beradi.

Anti-kriminalistik vositalarning birinchi toifasidan qolgan izlarilarini o‘chirilishi yoki cheklanganligiga har doim ham ishonch hosil qilishi mumkin emas. 2-toifalidagi vositalardan foydalanish aniq qayd etilmasligi mumkin. Ayniqsa, foydalanilgan jarayon umumiy operatsion funksiya bo‘lsa, masalan, disk tarixidan foydalanish jurnallari cheklangan bo‘lishi mumkin.

Muayyan vosita yoki jarayon uchun anti-kriminalistika vositalarni aniqlash amaliyotchiga quyidagi imkoniyatlarni beradi.

birinchi, amaldagi vositalar sinfini aniqlash – ya’ni, anti-kriminalistik vositalar izlaridan gumonlanuvchi tomonidan foydalaniladigan vositalar turini aniqlash (o‘chirish, ma’lumotlarni zararlash va h.k.).

ikkinchi, vositalarning kichik sinfini va individual xususiyatlarini aniqlash. Ba’zi hollarda foydalanilgan vositani aniqlash uchun uni platformada mavjudligini (hali o‘chirilmagan) tekshirish kerak. Bu har doim ham bo‘lmasligi mumkin. Bundan tashqari, aniqlanishi mumkin bo‘lgan vosita/jarayonning qanday ishlashi bo‘yicha ma’lum cheklovlar/zaif ham bo‘lishi mumkin. Bu tekshiruv davomida barcha dalillar topilishi va to‘g‘ri talqin qilinishini ta’minlash uchun muhim. Masalan, anti-kriminalistik vositalardan foydalanish holatini aniqlashda tizimda qanday vositadan foydalanilganligi yoki foydalanilmaganligini ko‘rsatish mumkin.

Ma’lumotlar o‘chirilgan taqdirda anti-kriminalistika vositalaridan qolgan izlar orqali o‘chirilishi kerak bo‘lgan ma’lumotlarning joylashuvi yoki turini aniqlash mumkin.

Ma’lumotlar manipulyatsiya qilingan taqdirda esa ushbu vositalaridan qolgan izlar oqali ishonchliligi tasdiqlanmagan ma’lumotlarni aniqlash mumkin.

Anti-kriminalistik vositalardan qolgan izlar tahlili orqali gumonlanuvchi harakatlarini aniqlash mumkin. Belgilar, masalan, fayllarni xavfsiz o‘chirish muayyan fayl tizimining metama’lumotlarini o‘zgarishiga olib kelishi mumkin. Bu “X” ilovasi yordamida fayllarni o‘chirish aktiga mos keladi. O‘z navbatida, bunday izlarni tahlil qilish orqali ma’lum dalil turini topish imkoniyati nima uchun yo‘qligigi tushuntirishi mumkin.

Anti-kriminalistik vosita maqsadini aniqlash qiyinchilik tug‘dirsada, bu amaliyotchilarga raqamli dalillar tarkibini yoki ma’lumotlarni buzish yoxud buzishga uringanligini aniqlash uchun ko‘proq imkoniyat beradi.

Gumon qilinuvchining noqonuniy xatti-harakatlarini aniqlashga yordam berish uchun raqamli kriminalistika inventarizatsiya jarayonlarini buzishi mumkin bo‘lgan vositalarning ta’sirini tekshirishi va qayd etishi zarur. Shunday qilib, soha ushbu vositalarning imkoniyatlarini va ulardan tizimda foydalanish xususiyatlarini aniqlash va baholashga yordam beradigan resursni ishlab chiqishni boshlashi zarur. Bu dalillarni ishonchliligi buzilgan holatlarda tizimdagi “yetishmayotgan” ma’lumotlarni tushuntirishga yoki kontentni ajratib ko‘rsatishga yordam beradi.

References:

1. Pajek, P. and Pimenidis, E., Computer anti-forensics methods and their impact on computer forensic investigation. In International Conference on Global Security, Safety, and Sustainability. Springer, Berlin, Heidelberg. 2009, September. pp. 145-155
2. Carriyer (2006) The Sleuth Kit [online] http://www.sleuthkit.org/index.php
3. https://www.linux.com/news/sandstorm-launches-netintercept-11-freebsd-forensics-and-analysis-tool/
4. Ushbu vositalarga tarmoq trafigi, TEMP ma’lumotlari, Web barouzer seanslari, Clipboard malumotlari va h.k.kiradi
5. Li u and Brown (2006), “Bleeding-Edge Anti-Forensics,” Infosec World Conference & Expo, MIS Training Institute.
6. Buskrik and Liu (2006), “Digital Evidence: Challenging the Presumption of Reliability”, Journal of Digital Forensic Practice, 1:19—26, 2006.
7. Conlan, K., Baggili, I. and Breitinger, F., 2016. Anti-forensics: Furthering digital forensic sciyence through a new extended, granular taxonomy. Digital investigation, 18, pp. S66-S75.
8. Al Fahdi, M., Clarke, N.L. and Furnell, S.M., 2013, August. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In Information Security for South Africa, 2013 (pp. 1-8).
9. Said, H., Al Mutawa, N., Al Awadhi, I. and Guimaraes, M., Forensic analysis of private browsing artifacts. In Innovations in information technology (IIT), International conference on. 2011, April. pp. 197-202.
10. Al Fahdi, M., Clarke, N.L. and Furnell, S.M., 2013, August. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In Information Security for South Africa, 2013 (pp. 1-8).

11. Kessler, G.C., Anti-forensics and the digital investigator. In Australian Digital Forensics Conference. 2007, March. p. 1.
12. . Harris, R. (2006). Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem. Proceedings of the 2006 Digital Forensics Research Workshop. Digital Investigation, 3(S), S44-S49. Retrieved September 11, 2007, from http://dfrws.org/2006/proceedings/6-Harris.pdf
13. Park, K.J., Park, J.M., Kim, E.J., Cheon, C.G. and James, J.I., Anti-Forensic Trace Detection in Digital Forensic Triage Investigations. Journal of Digital Forensics, Security and Law, 12(1), 2017. p.8.
14. Garfinkel, S., 2007, March. Anti-forensics: Techniques, detection and countermeasures. In 2nd International Conference on i-Warfare and Security (Vol. 20087, pp. 77-84).
15. Абдуллаев , Р. 2022. Проведение осмотра места происшествия с использованием передовых технологий. Общество и инновации. 3, 9/S (окт. 2022), 184–188. DOI:https://doi.org/10.47689/2181-1415-vol3-iss9/S-pp184-188.
16. Абдуллаев Рустам (2020). ПРАВОВЫЕ ВОПРОСЫ СБОРА И ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ. Review of law sciences, 3 (Спецвыпуск), 240-244. doi: 10.24412/2181-919X-2020-3-240-244
17. Abdullaev, R. (2023). JINOYATLARNI TERGOV QILISHDA ZAMONAVIY TEXNOLOGIYALARDAN FOYDALANISH. Theoretical Aspects in the Formation of Pedagogical Sciences, 2(9), 89–92. извлечено от http://www.econferences.ru/index.php/tafps/article/view/5983
18. Khamidov, B. K., & Ganiyev, O. T. (2022). DIGITAL FOOTPRINTS AND SOME QUESTIONS RELATED TO THEIR FORENSIC RESEARCH. Herald pedagogiki. Nauka i Praktyka, 2(4).