RAQAMLI KRIMINALISTIKA SOHASIDAGI ASOSIY MUAMMOLAR

Abduraximov Baxtiyor
O‘zbekiston Milliy universiteti, Toshkent
Allanov Orif,
Turdibekov Baxtiyor
Toshkent axborot texnologiyalari universiteti, Toshkent
Davlatov Mirzoulug‘bek
“QQQ-TECH” MChJ, Toshkent

Annotatsiya: *Raqamli kriminalistika kiberxavfsizlik uchun muhim soha bo‘lganligi bois tadqiqotchilar tomonidan katta e’tibor qaratilmoqda. Zamonaviy kiberhujumlarning tobora ortib borayotganligi to‘g‘ridan-to‘g‘ri dalillarni yig‘ishni qiyinlashtirayotganligi bilan bog‘liq va bu ko‘pincha bir nechta texnologiyalardan foydalanishni talab qiladi. Bugungi kunga qadar tadqiqotchilar ushbu sohada ko‘plab ilmiy ishlarni taqdim etishgan. Ushbu maqolada raqamli kriminalistika sohasiga tegishli ilmiy ishlar o‘rganib chiqilgan, raqamli kriminalistika bo‘yicha asosiy sohalar va ularning asosiy muammolari aniqlangan. Mavzular va usullarning xilma-hilligiga qaramay, ularning deyarli barchasi duch keladigan bir nechta umumiy muammolar mavjud. Ularning aksariyati qarshi tahlil usullari, qurilmalardan va bulutli tizimlardan ma’lumotlarni yig‘ish qiyinchiliklar tug‘dirmoqda. Texnik masalalardan tashqari, tadqiqot huquqiy, ilmiy va axloqiy masalalar bo‘yicha protsessual masalalarni hal qilish zarur isoblanadi. Tadqiqot ishidagi tahlil natijalarida raqamli ekspertizaning turli mavzulari bo‘yicha tadqiqotchilar va amaliyotchilarning natijalari keltirilgan.*

Kalit so‘zlar: *Raqamli ekspertiza, raqamli kriminalistika, kiberjinoyat, kriminalistika tekshiruvlari, kriminalistik muammolar.*

1. KIRISH

Raqamli kriminalistikada ko‘proq qiziqish raqamli dalillarga qaratiladi. Dastlab, asosiy faoliyat disklardan o‘chirilgan yoki yo‘q qilingan fayllarni tiklash uchun shaxsiy kompyuterlarni tekshirish bo‘lgan. 2000-yillarning boshidan boshlab, raqamli kriminalistika sohasi muntazam ravishda kengayib bormoqda[1]. Hozirgi vaqtda foydalanuvchilar bir nechta raqamli qurilmalardan va raqamli xizmatlardan foydalanishga moyildirlar[2]. Bizning kundalik hayotimizning raqamli izi juda katta hajmni egallaydi va shunga ko‘ra, noqonuniy harakatlar raqamli dalillarni to‘plashda turli qiyinchilik va muammolar keltirib chiqarmoqda. Kriminalistika ekspertlarga ehtiyoj ortmoqda va bu raqamli ekspertiza bilan bog‘liq ko‘plab ta’lim va sertifikatlash dasturlarini yaratishga undamoqda [3].

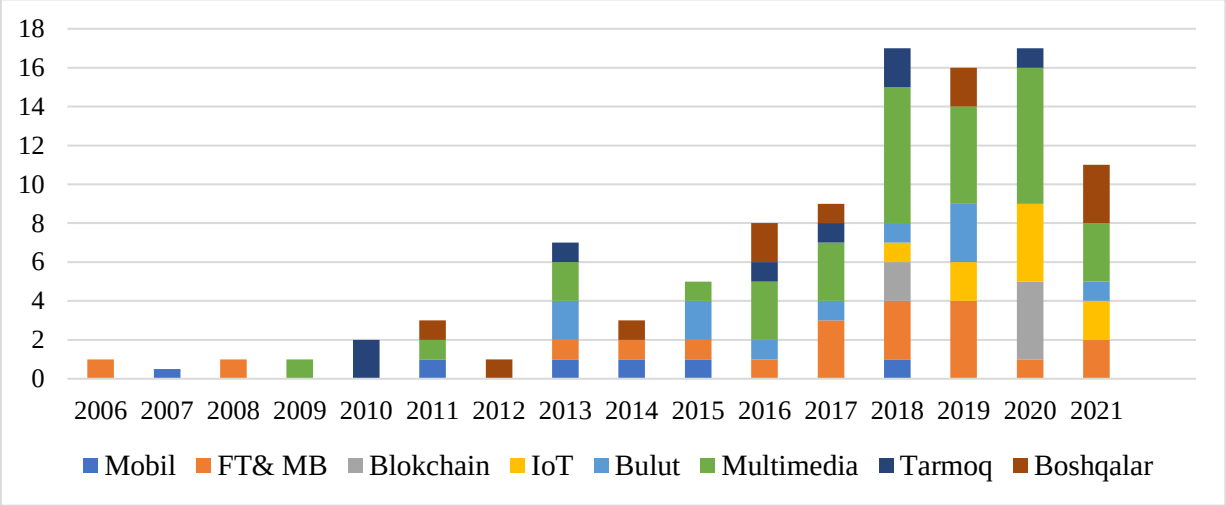
Kutilayotgan kiberjinoyatlarning kuchayishi bilan bir qatorda, raqamli dalillar deyarli barcha zamonaviy jinoyatlarni isbotlashga yordam beradi. Masalan, mobil qurilmalar raqamli dalillarning asosiy manbaiga aylandi, chunki foydalanuvchilarning deyarli barcha aloqalari ular orqali amalga oshiriladi[4]. Aslida, jinoiy tergovlarning asosiy qismi (85%) elektron dalillarni o‘z ichiga oladi. Shunday qilib, elektron pochta xabarlari, bulutli xizmat ko‘rsatuvchi provayderlar, onlayn to‘lovlar va olib yuriladigan qurilmalar ko‘pincha turli vaziyatlarda raqamli dalillarni olish uchun ishlatiladi.

Raqamli kriminalistikadagi ba’zi printsiplar bir xil bo‘lishi mumkin biroq ularni barcha turdagi dalillarni to‘plashga qo‘llab bo‘lmaydi. Misol uchun, bulutdan dalillar to‘plash IoT qurilmalari kriminalistikasiga yoki multimedia raqamli ekspertizasiga o‘xshamaydi. Bu har bir sohada ko‘tarilgan muammolarni alohida hal qiladigan katta miqdordagi tadqiqotlarga olib keladi.

Shuning uchun tadqiqot ishining asosiy qismi turli xil manbalardan raqamli dalillari olish uchun yangi vositalar va algoritmlarni ishlab chiqishga bag‘ishlangan.

2. RAQAMLI KRIMINALISTIKADA ASOSIY TADQIQOTLAR

Raqamli kriminalistika sohasidagi nashrlarning vaqt bo‘yicha taqsimlanishi 1-rasmda tasvirlangan. Ta’kidlash joizki, 2017 yildan keyin ushbu sohadagi tadqiqot ishlari soni sezilarli darajada oshdi. Shuni ta’kidlash kerakki, tadqiqot natijasida raqamli ekspertiza bo‘yicha 7 ta quyidagi yo‘nalishlar keng tarqalganligi aniqlandi: blokcheyn, bulutli xizmatlar, fayl tizimi va ma’lumotlar bazalari, multimedia, IoT, mobil va tarmoq kriminalistikasi. Multimedia kriminalistikasi hozirgi raqamli kriminalistika tadqiqotlarining eng ko‘p qismini o‘z ichiga oladi, undan keyin fayl tizimi va ma’lumotlar bazasi ekspertizasi o‘rin olgan. Ikkala soha ham oson saqlash va uzatish qobiliyatini oshiradigan mobil qurilmalarning keng qo‘llanilishi multimedia bilan bog‘liq kontentning katta generatsiyasiga olib kelganligini ko‘rsatadi. Bundan



1-rasm. Raqamli kriminalistika turli sohalaridagi tadqiqotlarning yillar bo‘yicha taqsimoti

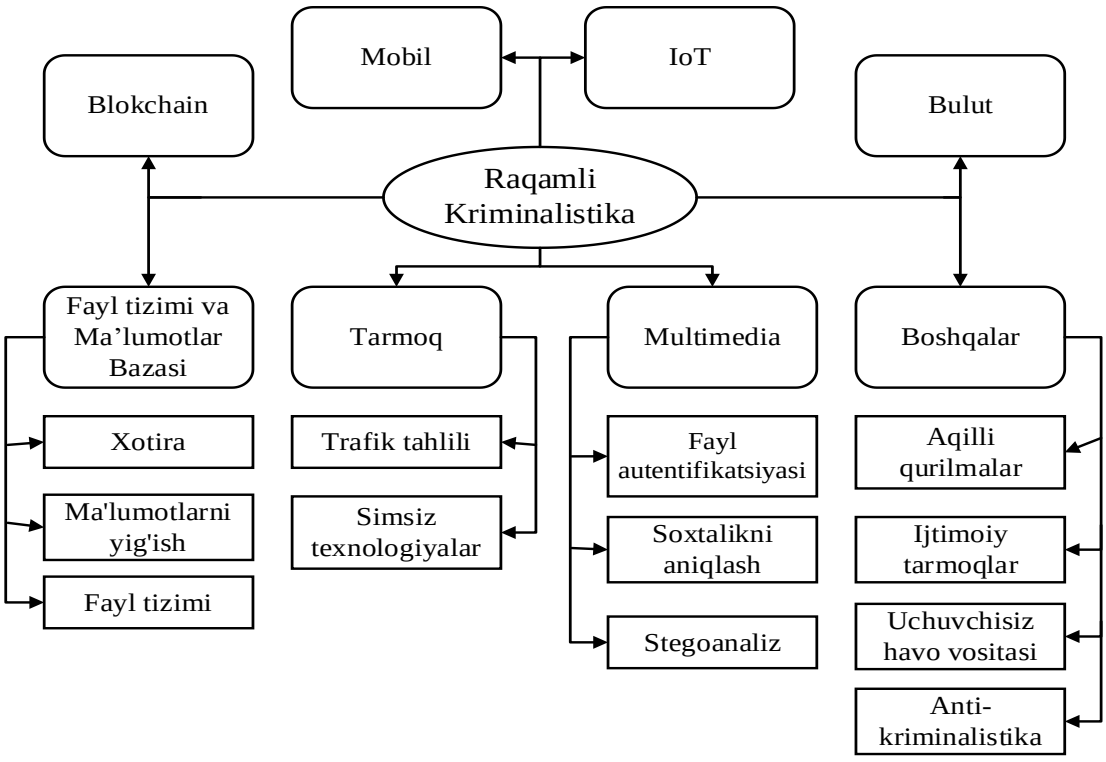
tashqari, turli xil tahlil hujjatlarda (yuqoridagi toifalarning birortasiga to‘g‘ri kelmaydigan) raqamli kriminalistikaning ko‘p tarmoqli xususiyatini ko‘rsatadi. Ushbu ko‘p tarmoqli sharhlar ijtimoiy media, aqlli tizimlar va qurilmalar, uchuvchisiz havo vositalari va boshqa shu kabi sohalarda olib borilgan tadqiqotlarni aks ettiradi.

Raqamli ekspertiza mavzularining tasniflanishini quyidagi 2-rasmdagi kabi tasvirlash mumkin. Har bir holatda adabiyotlarda taklif qilingan asosiy muammolar muhokama qilingan.

Bulutli hisoblash. Tadqiqotchilar, shuningdek, davlat idoralari bulutli hisoblash ekspertizasidagi ko‘plab muammolarni chuqur o‘rganib chiqishgan, ammo ba’zi muammolar hali ham hal qilinishi kerak. Misol uchun, ishlash muddati qisqaroq bo‘lgan o‘rnatilgan operatsion tizimlarning xilma-xilligi, shuningdek, butun dunyo bo‘ylab mavjud bo‘lgan ko‘plab smartfon ishlab chiqaruvchilari ushbu tadqiqot sohasidagi muammolar hisoblanadi. Aleks va boshqalar[5] bulutli hisoblash ekspertizadagi ma’lumotlarni yig‘ish, ro‘yxatga olish, bulutli xizmat ko‘rsatuvchi provayderlarga qaramlik, jinoyat joyini qayta qurish, transchegaraviy qonun va qonun taqdimoti bilan bog‘liq muammolarni keltirishgan. Khanafseh va boshqalar[6] bulutli hisoblash ekspertizadagi quyidagi muammolarni ta’kidlaganlar:

– jurnallar formatini birlashtirish;

– foydalanuvchi va bulutli xizmat ko‘rsatuvchi provayder o‘rtasidagi xizmat ko‘rsatish darajasi to‘g‘risidagi kelishuvda etishmayotgan shartlar;



2-rasm. Raqamli kriminalistikaning asosiy sohalari klassifikatsiyasi

– kriminalistika ma’lumotlariga kirishning kamayishi va mijoz tomonidan barcha darajadagi ekspertiza ma’lumotlarini nazorat qilish;

– xalqaro hamkorlik va ma’lumotlarga kirish va almashishda xalqaro hamkorlik va qonunchilik mexanizmining yo‘qligi;

– ma’lumotlarga kirish va almashishda xalqaro hamkorlik va qonunchilik mexanizmining etishmasligi.

Tarmoq kriminalistikasi. Ma’lumotlarni monitoring qilish va tarmoq trafigidan olish hozirgi kundagi kiberhujumlarning ko‘pchiligini oldini olish uchun zarurdir [7], jumladan, xizmat ko‘rsatishni rad etish (DDoS), fishing, DNS tunnellash, Man-in-the-middle (MitM) hujumlari, SQL in’ektsiyasi va boshqalar[8].

Ularning orqasida turgan mexanizmdan qat’i nazar (tajovuzkorlar yoki botnetlar), tahlil qilish va yumshatish mexanizmlari, dalillar va har qanday hujumni aniqlash yoki zaiflikni isbotlash uchun kompyuter tarmog‘i trafigining to‘g‘ri monitoringi va tahliliga tayanadi. Ushbu maqsadga qaratilgan bir qancha vositalar mavjud. Masalan, trafikni aniqlash, hujumlarni aniqlash tizimlari (IDS), protokol tahlili va xavfsizlik hodisalarini boshqarish (SEM) kabi funksiyalarni ta’minlovchi tarmoq kriminlistikasi vositalari. Shunga qaramay, tarmoq kriminalistikasining vazifalaridan biri shifrlangan tarmoq trafigida paketlarni aniq va samarali tahlil qilishga erishishdir, chunki bu shifrlanmagan trafikni tahlil qilishdan ancha qiyin. Mualliflar [9] da ta’kidlaganidek, paketli tahlilda mashinali o‘qitishdan foydalanish noma’lum xususiyatlar va shifrlangan tarmoq ma’lumotlar oqimlarini tahlil qilishga qaratilgan murakkab tadqiqot sohasiga aylanib bormoqda.

Mobil kriminalistika. Smartfonlar va mobil qurilmalar ko‘plab tergov maqsadlari uchun qimmatli ma’lumotlarni olishga imkon beradi. Mobil kriminalistika (MK) raqamli ekspertiza yo‘nalishidagi mobil qurilmalardan raqamli dalillarni olish bilan bog‘liq bo‘lgan sohadir.

Ishlash muddati qisqaroq bo‘lgan o‘rnatilgan operatsion tizimlarning xilma-xilligi, shuningdek, butun dunyo bo‘ylab ko‘plab smartfon ishlab chiqaruvchilari MK sohasidagi muhim muammolar sifatida ajralib turadi. Umuman olganda, MK ko‘p sabablarga ko‘ra turli xil muammolarni keltirib chiqaradi. Masalan, [10] mualliflar MK tekshiruvlarini muvaffaqiyatli o‘tkazish uchun quyidagi muammolarni aniqlashgan:

– ma’lumotlar bilan bog‘liq muammolar (anonimlik bilan bog‘liq bo‘lgan ko‘rish va boshqa anonimlik xizmatlari va tergov davomida olingan katta hajmdagi ma’lumotlar);

– raqamli ekspertiza vositalar bilan bog‘liq muammolar;

– qurilma va operatsion tizimlarning xilma-xilligi;

– xavfsizlik jihatlari (ishlab chiqaruvchilarning yangi va yanada murakkab raqamli ekpertizaga qarshi usullarini ishlab chiqish);

– bulut bilan bog‘liq muammolar (hozirgi MK vositalari bulutli jihatlarni, bulutli tergov to‘siqlarini, masalan, huquqiy bazalar tufayli kriminalistika ma’lumotlariga kirish, kriminalistika ma’lumotlarining xavfsizligini hisobga olinmasligi);

– jarayonlarni avtomatlashtirish.

Shuni ta’kidlash kerakki, MK umumiy jarayonlariga e’tibor qaratish bilan bog‘liq jiddiy muammolarga duch keladi. Misol uchun, tergov protseduralari har bir qurilma uchun modelga xos bo‘lishi kerakligi yoki kriminalistika protseduralariga qo‘llaniladigan standartlashtirilgan ko‘rsatmalar to‘plamini shakllantirish uchun etarlicha umumiy bo‘lishi kerakligi bilan bog‘liq muammolar.

Yana bir qiyinchilik - bu real vaqtda raqamli ekspertiza o‘tkazish zarurati (mobil qurilma yoqilgan bo‘lishi kerak) [11]. Bundan tashqari, MK tekshiruvlarini real vaqtda o‘tkazish uchun muhim to‘siq smartfonlarning turli xil tarmoq imkoniyatlari bilan bog‘liq bo‘lib, bu umumiy MK jarayonlarini boshqarishni qiyinlashtiradi, ayniqsa bulutli hisoblash muhitining murakkab tuzilishi tufayli vujudga keladi. Va nihoyat, zamonaviy mobil qurilmalarga xos bo‘lgan xavfsizlik choralari tufayli ekspert qurilma ma’lumotlarini o‘zgartirishi mumkin bo‘lgan ekspluatatsiya yordamida qurilmaga kirishi kerak bo‘ladi.

IoT qurilmalar kriminalistikasi. IoT qurilmalari va IoT bilan bog‘liq ilovalarning keng qo‘llanilishi xavfsizlik va kriminalistika sohasida yangi muammolarni keltirib chiqardi. IoT kriminalistikasi IoT bilan bog‘liq kiberjinoyatlar bilan shug‘ullanadigan raqamli ekspertiza bo‘limi bo‘lib, ulangan qurilmalar, sensorlar va barcha mumkin bo‘lgan platformalarda saqlanadigan ma’lumotlarni tekshirishni o‘z ichiga oladi.

IoT qurilmalar kriminalistikasida bir qancha ma’lumotlar manbalarining turli oqimlarini boshqarish, IoT ning murakkab uch bosqichli arxitekturasi, real vaqt rejimida jurnallarni olish va ularni amaldagi yagona shaklda saqlash uchun standartlashtirilgan tizimlarning yo‘qligi, to‘plangan barcha ma’lumotlar to‘g‘risida batafsil hisobotlarni tayyorlash, ma’lumotlarning o‘zgaruvchanligi va qiymatini hisobga olgan holda dalillarni saqlash va IoT ekotizimida odatiy ekspertiza vazifalarni qabul qilish[12]. Ma’lumotlarni shifrlash tendentsiyalari IoT kriminalistika ekspertlari uchun qo‘shimcha qiyinchiliklar tug‘diradi. Kriptografik himoyalangan saqlash tizimlari samarali raqamli ekspertiza tahliliga to‘sqinlik qiluvchi eng muhim to‘siqlardan biridir[13]. Boshqa tadqiqotlar IoT qurilmalar kriminalistikasi jarayonlarining qo‘shimcha cheklovlarini ta’kidlaydi. Masalan, ulangan IoT qurilmalarining katta miqdori bilan bog‘liq o‘zaro muvofiqlik va mavjudlik

muammolari[14], IoT ekspertiza dalillarining Big Data tabiati (turlilik, tezlik, hajm, qiymat, haqiqiylik) va IoT kriminalistika dalillarini saqlashning turli xil muammolari[15].

Ma'lumotlar bazasi kriminalistikasi. Katta fayl tizimlarining kriminalistik tahlili potentsial katta hajmdagi fayllar va ulardagi ma'lumotlarni boshqarishning samarali usullarini talab qiladi. Tizim jurnallari raqamli ekspertizadan foydalanish uchun eng ko‘p foydalaniladigan axborot manbalaridan biridir. Tizim xotirasida tizimdan foydalanish bilan bog‘liq dalillar, jumladan, ishlaydigan jarayonlar ro‘yxati, tarmoq ulanishlari yoki drayverni shifrlash kalitlari bo‘lishi mumkin. Odatda, bunday ma'lumotlar tizimning doimiy xotirasida saqlanmaydi va tizim o‘chirilganda yoki elektr tarmog‘idan uzilganda butunlay yo‘qoladi. Xotira qurilmalaridagi ma'lumotlarni yig‘ish usullari [16] (ya'ni, apparat va dasturiy ta'minotga asoslangan), tahlil qilish [17] va mavjud vositalar tahliliga bag‘ishlangan tadqiqotlarni ko‘plab uchratish mumkin. Ma'lumotlar bazasi ekspertizasining asosiy muammolari xotiraning o‘zgaruvchanligidan kelib chiqadi, shuning uchun uni tizim ishlayotgan paytda olish kerak. Chunki ma'lumotlar ishlayotgan ilovalarda o‘zgartirilishi mumkin. Bu ma'lumotning buzilish muammosiga olib kelishi mumkin ya'ni xotira qurilmasidagi ma'lumotning haqiqiy tarkibi bilan solishtirganda jadvallarda tasvirlangan xotira holati o‘rtasidagi nomuvofiqlik bo‘lishi mumkin. Xotira qurilmasidagi ma'lumotni yig‘ish jarayonida yuzaga kelishi mumkin bo‘lgan yana bir muammo - sahifalarni almashtirish yoki talab qilingan sahifalar tufayli xotirada mavjud bo‘lmagan sahifalarni birlashtirishdir. Va nihoyat, xotirani yig‘ish texnikasi operatsion tizim va apparat ko‘rinishida bo‘lishi kerak bo‘lsada, har bir operatsion tizim arxitekturasi xotira qurilmasini boshqacha boshqaradi va unga kirishga to‘sqinlik qiluvchi o‘ziga xos buzishdan himoya qilish mexanizmlari bilan jihozlangan bo‘ladi.

Ma'lumotlar bazasi (MB) ma'lumotlarni tartibga solish va saqlashning eng an'anaviy usuli hisoblanadi. Aksariyat ilovalar va onlayn xizmatlar o‘z mijozlari, moliyaviy qaydlar, inventar va boshqalar haqidagi yozuvlarni saqlash uchun ma'lum turdagi ma'lumotlar bazasidan foydalanadi.

MB da bo‘lishi mumkin bo‘lgan katta hajmdagi ma'lumotlardan tashqari, foydalanuvchilarga ma'lumotlar bazasini boshqarish va ma'lum formatda ma'lumotlarni saqlash va ulardan foydalanish imkonini beruvchi ma'lumotlar bazasini boshqarish tizimi (MBBT), shuningdek, foydalanuvchi darajasidagi harakatlarini isbotlashi mumkin. Masalan, u ma'lum qaydlar kim va qachon saqlanganini va ularga kirganligini ko‘rsatishi mumkin. Shu sababli, MB uchun raqamli kriminalistika tadqiqot hamjamiyatining e'tiborini tortgan[18]. Shu nuqtai nazardan, bir qancha tadqiqot ishlari relatsion va NoSQL MB uchun jurnal fayllari, metama'lumotlar va

shunga o‘xshash turdagi artefaktlar asosida ma’lumotlar bazasining raqamli kriminalistkasiga qaratilgan. Bundan tashqari, boshqa mualliflar ma’lumotlarni yig‘ish va tahlil qilish tartibi bo‘yicha raqamli kriminalistika imkoniyatlarini, shuningdek, kriminalistika protseduralaridan foydalanish uchun ularning tizimli arxitekturasini ko‘rib chiqilgan.

Blokcheyn tizimlari kriminalistikasi. Blokcheyn texnologiyasi doimiy ravishda mavjud tizimlarga integratsiya qilingan yoki turli sohalarda tizimlarni noldan tiklash uchun asos sifatida ishlatilgan. Dastlab qo‘llanilgan moliyaviy domendan tashqari, bitkoin orqali blokcheyn texnologiyasi hozirda ta’minot zanjirini boshqarish, kiberxavfsizlikni yaxshilash, hujjatlar, sertifikatlarni tekshirish va boshqalar kabi turli xil holatlarida qo‘llaniladi. Bundan tashqari, blokcheynga o‘rnatilgan moliyaviy tizim an’anaviy to‘lov tizimlariga qaraganda ko‘proq maxfiylikni ta’minlaganligi sababli, kriptovalyutalarning jinoiy faoliyat uchun ishlatilishi odatiy holdir. Bu blokcheyn tizimlarida saqlanadigan katta hajmdagi ma’lumotlar va bunday tizimlar tomonidan boshqariladigan jarayonlar soni tufayli blokcheyn tizimlari kriminalistikasi metodologiyasini zarurat sifatida belgilaydi[19]. Blokcheynga asoslangan tizimlarning asosiy xususiyati raqamli ekspertiza bilan bevosita bog‘liq bo‘lgan ma’lumotlar yaxlitligini kafolatlangan himoya qilishdir.

Shuni ta’kidlash kerakki, blokcheyn tizimlarining katta qismi ommaviy bo‘lib, hamma uchun kirishga imkon beradi va shu bilan kriminalistika tahlilini ortiqcha jarayonga aylantiradi. Kompyuter eksperti umumiy blokcheyn tarmog‘ida tugunni o‘rnatishi, uni qolgan tugunlar bilan sinxronlashtirishi va jurnalning mahalliy nusxasini olishi mumkin. Bunday hollarda ham, blokcheyn tizimlari jurnalida saqlanadigan ma’lumotlarning tuzilishi barcha kerakli ma’lumotlarni olish uchun maqbul emas (masalan, ma’lum bir hisob yoki maxsus smart-kontrakt uchun), shuning uchun jamoat jurnallarida saqlanadigan katta hajmdagi ma’lumotlardan qimmatli ma’lumotlarni ajratib olish uchun samarali mexanizmlar talab qilinadi. Xususiy blokcheyn tizimlarida, bugalteriya hisobi ma’lumotlari ommaga ochiq emas va ma’lumotlarni olish uchun blokcheyn tugunlariga an’anaviy raqamli ekpertiza yondashuvlarini qo‘llash kerak.

Buxgalteriya hisobida saqlangan ma’lumotlar katta ahamiyatga ega bo‘lsada, blokcheyn tugunini tahlil qilishda ko‘proq ma’lumotlarga e’tibor berish kerak. Bugalteriya hisobida barcha tuzilgan tranzaktsiyalar saqlanadi, ammo blokcheyn tugunlari boshqa tugunlar yoki mijozlar bilan o‘zaro aloqalari haqida ko‘proq ma’lumotni saqlaydi. Masalan, tranzaktsiyani yuborish uchun tugunga ulangan mijozning IP-manzili yoki tarmoqdagi muayyan tugunning faoliyati (masalan, sinxronlash so‘rovlari) bilan bog‘liq bugalteriya ma’lumotlari. Bundan tashqari, bir

nechta xavfsizlik blokcheyn hujumlari asosan uning tarkibiga emas, balki infratuzilmaga yoki tarmoqning magistraliga qarshi qaratilgan bo‘ladi.

Multimedia ma’lumotlar kriminalistikasi. 4-sanoat inqilobi tomonidan qo‘llanilgan hamma joyda keng tarqalgan texnologiyalar (masalan, IoT qurilmalari, smartfonlar, olib yuriladigan qurilmalar) sonining ko‘payishi, shuningdek, 5G texnologiyasi orqali aqlli senariylarda ulanish imkoniyatlarining sezilarli darajada yaxshilanishi tufayli, multimedia ma’lumotlarni ishlab chiqaruvchilar va iste’molchilari soni yildan-yilga keskin ortib bormoqda. Bir tomondan, bu sanoat kompaniyalar va foydalanuvchilar uchun imkoniyatdir. Boshqa tomondan u zararli foydalanuvchilar foydalanishi mumkin bo‘lgan bunday tizimlarning mumkin bo‘lgan zaifliklari va hujumlari sonini oshiradi.

Multimedia kontentida raqamli ekspertizani amalga oshirish tadqiqotchilar e’tiborini tortmoqda. Global nuqtai nazardan tasvirlar soxtaligini aniqlash tadqiqotlari ko‘plab mavjud. Shu nuqtai nazardan, pikselga asoslangan tasvirni soxtalashtirishni aniqlash asosiy mavzulardan biridir. Tasvirni birlashtirish soxtaligi va nusxa ko‘chirish soxtaligi unda joriy tasvirlarning qismlari o‘ziga xos xususiyatlarni biriktirish va yashirish uchun ishlatiladi. Boshqa multimedia raqamli ekspertizasi tadqiqotlarida giperspektral tasvir, tasvir autentifikatsiyasi, tasvirlardagi shovqin ta’siri va tasvir steganalizi [21] kabi mavzularni tahlil qilishgan.

Tadqiqotlarning yana bir to‘plami bolalarga nisbatan zo‘ravonlik materiallarini tasvir va video tahlillar orqali aniqlashga qaratilgan. Hozirda chuqur o‘rganish usullarining paydo bo‘lishi tasvirning yaxlitligini aniqlash va tekshirish imkoniyatlarini oshirdi. Bu tasvir bilan bog‘liq bir qancha vazifalarda, ayniqsa, raqamli ekspertizaga qarshi vositalar ishlatilganda an’anaviy usullardan ustun keladi[22].

Boshqa turli sohalar. Ushbu bo‘lim oldingi paragraflarning nom toifalaridan tashqarida bo‘lgan raqamli ekspertiza sharhlariga bag‘ishlangan. Anti-kriminalistika atamasi kriminalistika ekspertlari va ularning vositalarini o‘z maqsadlariga erishishga to‘sqinlik qiladigan usullar va strategiyalarni anglatadi. Raqamli ekspertizaga qarshi metodologiyalarning bir nechta turlari mavjud. Masalan, shifrlash, ma’lumotlarni yashirish(izni yashirish), dalillarni o‘chirish, steganografiya va tasvirni buzish, himoyalangan yashirin aloqalar (masalan, tunnelli aloqa), zararli dasturlarga qarshi muhiti, spoofing va umumiy tahlilga qarshi usullar. Raqamli ekspertizaga qarshi usullar inson elementlarining kriminalistika vositalariga bog‘liqligidan, arxitektura va hisoblash quvvati nuqtai nazaridan va asosiy uskunaning cheklovlaridan foydalanadi. Shu sababli, ekspertlarning tayyorgarligi va bilim darajasini oshirish va yanada mustahkam raqamli ekspertiza tartib-qoidalarini yaratish ekspertizaga qarshi ta’sirni minimallashtirish uchun juda muhimdir. Ushbu yo‘nalishda ba’zi mualliflar raqamli

ekspertiza modellaridan foydalanish raqamli ekspertizaning mustahkamligini oshirishga yordam berishini ta’kidlaydilar [23].

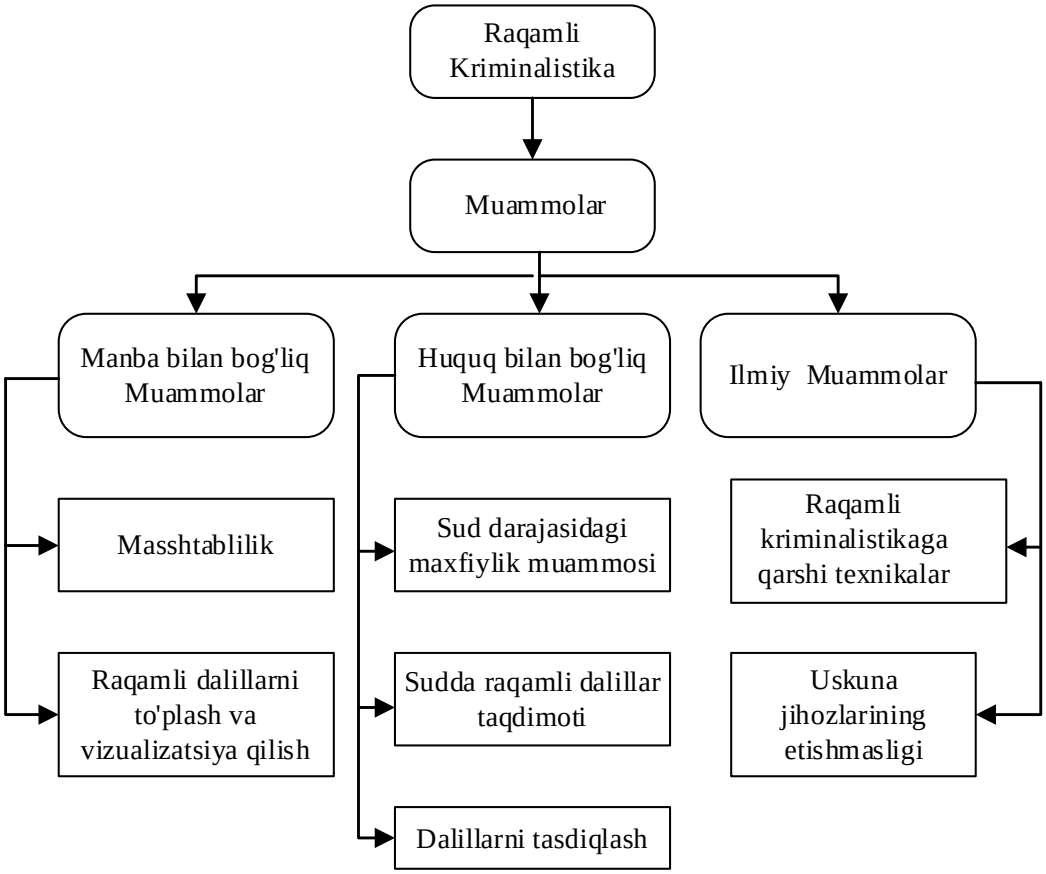
Raqamli kriminalistikada paydo bo‘lgan yana bir mavzu uchuvchisiz havo vositalari (UAV yoki dronlar deb nomlanadi) bilan bog‘liq [24]. Ushbu qurilmalarning ko‘p qirraliligi sanoatdan tortib harbiy ilovalargacha bo‘lgan ko‘plab kontekstlarda mashhur bo‘lib bormoqda. Dron kriminalistikasining asosiy muammolaridan biri dronning bir qismi bo‘lgan turli apparat komponentlari to‘plamidir. Masalan, dronlar sensorlar, parvoz boshqaruvchilari, elektron va apparat komponentlari, bort kompyuterlari va radiochastota qabul qiluvchilardan iborat bo‘lib, ularning har biri bir yoki bir nechta dalil manbalari bilan bog‘langan. Masalan, ma’lumotlarni saqlash (dronda mavjud bo‘lgan turli xil xotira manbalari, masalan, media yoki boshqa dasturiy ta’minotni saqlaydigan xotira kartalari), ma’lumotlar kommunikatsiyalari va boshqa jurnallar va dron bilan bog‘liq manbalarda saqlanadigan ma’lumotlar[25].

3. RAQAMLI KRIMINALISTIKA MUAMMOLARI

Hozirgi kunda kiberjinoyatlar kiberxavfsizlik bo‘yicha mutaxassislar uchun bir qator muammolarni keltirib chiqardi, ularning ba’zilari texnologiya yoki taraqqiyot bilan bog‘liq, ba’zilari standartlar va qoidalar bilan, ba’zilari esa tergovning asosiy funksionalligi bilan bog‘liq. Raqamli kriminalistikaning asosiy muammolarini asosan uchta asosiy qismga bo‘lish mumkin:

- Manba bilan bog‘liq muammolar;
- Huquq bilan bog‘liq muammolar;
- Ilmiy muammolar[26].

Manba bilan bog‘liq muammolar. Ushbu turdagi muammolar raqamli ekspertizada funksional muammolar tufayli yuzaga keladi, funksional muammolar voqeani tekshirish uchun ekspertlar tomonidan qabul qilinadigan asosiy muhit yoki harakatlar rejasi bilan bog‘liq. Raqamli kriminalistikadagi asosiy muammolar quyidagi 3-rasmda keltirilgan.



3-rasm. Raqamli kriminalistika muammolari

Masshtablilik. Masshtablilik raqamli tergovdagi ma’lumot hajmi bilan bog‘liq. Ba’zan, mutaxassis kerakli dalilni topishi uchun ma’lumotlarni to‘plashi va qayta ishlashi juda murakkab ishdir. Shunday qilib, ushbu turdagi muammolarni yumshatish uchun kiberjinoyat va tergovning hozirgi senariysiga mos keladigan vaqt belgisi bilan tuzilgan raqamli ekspertiza jarayonini yaratish kerak.

Raqamli dalillarni to‘plash va vizualizatsiya qilish. Bu raqamli kriminalistikaning yana bir muhim muammosi bo‘lib, hozirda ekspertlar tez-tez bu muammoga duch kelmoqda. U masshtablilikdan farq qiladi. Masshtablilik - bu dalillarni to‘plash va tahlil qilish vaqtidagi ma’lumotlar hajmidir. Bunda ekspertlar dalillarni zarar ko‘rgan tomonlar va yuristlar oldida o‘qilishi mumkin bo‘lgan tarzda to‘plash va vizualizatsiya qilish uchun ketadigan vaqtga e’tibor berishadi. Ma’lumotlarni shifrlash, steganografiya, ma’lumotlarni yashirish, defragmentatsiya va boshqalar kabi ilmiy muammolar tufayli ekspertlar odatdagidan ko‘proq vaqt sarflaydi. Bu raqamli kriminalistikada katta muammolarni keltirib chiqaradi va ba’zida ma’lumotlarni olish juda muhim va murakkab. Bu shuningdek, ma’lumotlarning buzilishi xavfiga olib keladi. Shunday qilib, ushbu texnik muammolarning barchasi

ma’lumotlarni to‘plash va vizualizatsiya qilishni ko‘p vaqt talab qiladigan jarayonga aylantiradi, buning natijasida keyingi tergov jarayoni ham kechiktiriladi. Ushbu turdagi muammolarni kamaytirish uchun yumshatish strategiyalari juda chalkash, chunki agar ekspert tezkor yig‘ish strategiyasini yaratsa, ma’lumotlarning buzilishi xavfi ortadi[27].

Huquq bilan bog‘liq muammolar. Ushbu turdagi masalalarda turli mamlakatlarda turli xil qonunlar mavjud va ba’zi mamlakatlarda hatto qonun yoki raqamli ekspertiza uchun belgilangan standartlar mavjud emas. Shunday qilib, raqamli ekspertiza va kiberxavfsizlik qonunlari bilan bog‘liq bir qancha noaniqliklar va muammolar mavjud. Misol uchun, agar tekshiruvchi voqea xorijiy davlatda joylashgan tizim tomonidan sodir etilganligini aniqlasa va u mamlakatda hech qanday kiber qonun yo‘q bo‘lsa ekspert hech narsa qila olmaydi va bu ekspertlar va ekspertlar uchun juda katta qiyinchilik tug‘diradi. Qonun bilan bog‘liq boshqa ko‘plab masalalar mavjud. Ba’zi asosiy muammolar quyida keltirilgan.

Sud darajasidagi maxfiylik muammosi. Ushbu turdagi masalalarda asosiy e’tibor shaxsiy daxlsizlikdir. Oddiy so‘z bilan aytganda, aksariyat hollarda mutaxassislar haqiqatni topish uchun tashkilot va shaxsga tegishli shaxsiy ma’lumotlarni oshkor qilishlari kerak. Shaxsiy foydalanuvchilarning 60% va korxonalarning 77% kundalik foydalanishda shaxsiy va maxfiy ma’lumotlardan foydalanishadi va agar ma’lumotlar ommaviy yoki tajovuzkorlarga oshkor etilsa, bu turdagi ma’lumotlar ular uchun xavf tug‘diradi.

Dalillarni tasdiqlash. Dalillarni tekshirish raqamli kriminalistikaning asosi bo‘lib, har qanday kiberjinoyatda hal qiluvchi rol o‘ynaydi. Sudda muxolifatchi advokat dalillarni tekshirishda foydalanilgan vositaga e’tiroz bildiradigan ko‘plab holatlar mavjud va bu raqamli kriminalistikada katta muammo tug‘diradi, chunki har bir vosita o‘zining ijobiy va salbiy tomonlariga ega. Shuning uchun ekspert qaysi vosita qaysi vazifaga mos kelishini topishda qiynaladi. Ko‘pgina mamlakatlarda ushbu muammodan keyin qonuniy kuchga ega vositalar ro‘yxati mavjud, ammo bu vositalarda kamchiliklar ham yo‘q emas. Har qanday vazifa uchun 100% mukammal vosita yo‘q va bu masala raqamli kriminalistikada muammo bo‘lib qolmoqda.

Ilmiy muammolar. Bugungi davrda ilmiy yoki texnik masalalar juda muhim, chunki zamonaviy texnologiyadan foydalanish yaxshi va yomon tomonlari mavjud. Buzg‘unchilar noqonuniy, ruxsat etilmagan faoliyatni amalga oshirish va anonim qolish uchun zamonaviy texnologiyalardan nomaqbul tarzda foydalanadilar. Texnologiya foydalanishning bunday turi ilmiy jihatdan muammo tug‘diradi va bu bugungi davrdagi eng xavfli masaladir. Asosan ikkita turdagi muammolar mavjud, ular quyidagicha tavsiflanadi.

Ma'lumotlarni shifrlash. Bu foydalanuvchilar tomonidan qo'llaniladigan odatiy jarayon, ammo buzg'unchi shaxslar ham o'zlarining ma'lumotlarini raqamli ekspertlardan yashirish uchun ushbu usuldan foydalanadilar. Ma'lumotlarni shifrlash uchun turli xil bepul vositalar mavjud va shuning uchun bu kriminalistika eksperti duch keladigan juda keng tarqalgan muammo. Ba'zan oddiy vositalar yordamida ma'lumotlarni shifrlash oson, ammo ma'lumotlarning shifrini ochish ekspert uchun juda muhim va murakkab. Chunki turli xil shifrlash algoritmlari mavjud va ba'zilari juda murakkab, shuning uchun ekspert uchun algoritmni aniqlash va deshifrlash ko'proq vaqt talab etadi.

Saqlash maydonida ma'lumotlarni yashirish. Ba'zida tajovuzkor dalillarni yashirishga harakat qiladi, shuning uchun tajovuzkorlar fayllar yoki ma'lumotlarni saqlash muhitiga yoki boshqa joyga yashiradilar. Buzg'unchilar bu turdagi ma'lumotlarni qandaydir maxsus texnika bilan yashirishadi, shuning uchun oddiy yoki klassik xotira qurilmasi kriminalistik vositalari ularni topa olmaydi. Ba'zida noma'lum xotira qurilmasidan ma'lumotlarni olish juda murakkab va xavfli bo'lib, ma'lumotlar buzilishiga olib keladi.

Steganografiya. Hozirgi sharoitda raqamli kriminalistikaga qarshi turishning eng mashhur va qiyin usuli steganografiya hisoblanadi. Steganografiya - bu fayl, video yoki har qanday multimediadagi ba'zi ma'lumotlarni yashirish jarayoni. Oddiy so'z bilan aytganda, Steganografiya juda keng qo'llaniladigan usuldir, chunki internetda CryptApp, Shadow, Crypsis va boshqalar kabi bepul steganografiya uchun ko'plab vositalar mavjud.

Uskuna jihozlarining yetishmasligi. Bu raqamli kriminalistikada juda muhim masala, chunki raqamli ekspertiza jarayonida apparat jihozlarining yetishmasligi mavjud. Raqamli kriminalistikaning ayrim sohalari ham borki, ular uchun apparat hali ishlab chiqarilmagan. Raqamli kriminalistika tekshiruvida apparat muhim ro'l o'ynaydi, chunki apparat yordamida ekspert o'z vaqtida kechiktirmasdan to'g'ri ishlaydi.

4. TAHLIL VA UMUMLASHTIRISH NATIJALARI

1-jadvaldan ko'rinib turibdiki eng ko'p e'tirof etilgan muammo - bu turli xil manbalardan (ma'lumotlar va qayd yozuvlarni dinamik ravishda to'playdigan turli xil apparat va monitoring vositalari) ma'lumotlarni olish va uni talqin qilishdir. Ma'lumotlarni yig'ish va boshqarish raqamli ekspertiza bilan bog'liq faoliyatga ta'sir qiladigan muammodir. Shuni ta'kidlash kerakki, ma'lumotlarni yig'ish tadqiqotchilar va amaliyotchilarga o'z modellarini baholashda va yaratishda juda muhimdir va bu raqamli kriminalistika texnologiyalari va vositalarining rivojlanish sur'atiga turtki

beradi [28]. Keyingi eng qiyin masala raqamli ekspertizaga qarshi usullar bilan bog‘liq. Bu buzg‘unchi shaxslar tomonidan qo‘llaniladigan raqamli ekspertizaga qarshi

1-jadval. Turli sohalarda mavjud raqamli kriminalistika muammolari

Muammolar	Bulut	Tarmoq	Mobil	IoT	FT&MB	Blokcheyn	Multimedia
Turli joyda saqlanadigan manbalardan ma’lumotlarni olish	●	●	●	●	●		●
Raqamli ekspertizaga qarshi va himoyalangan saqlash tizimlari	●		●	●	●	●	●
To‘g‘ri va standartlashtirilgan baholash mezonlari				●	●	●	●
Turli tergov senariylari uchun yuridik va qonuniy talablarning yo‘qligi	●		●	●			
Raqamli ekspertizaga tayyorgarlik mexanizmlarining yo‘qligi	●			●			●
Yangi kiberjinoyatlarga qarshi kurashish uchun raqamli kriminalistika vositalarini yangilash	●		●	●			●
Ekspertlar va sud o‘rtasida o‘qitish va o‘zaro hamkorlikning yo‘qligi	●			●	●		
Oldindan ishlov berish, o‘qitish va ma’lumotlarni yig‘ish uchun qo‘shimcha xarajatlar sarfi		●	●			●	●
Turli yuridik qonunlar tufayli chegaraviy tekshiruvlar	●			●			
Qurilmaga asoslangan standartlar va ko‘rsatmalarning yo‘qligi			●		●		
Real vaqtda tahdidlarni va hujumlarni ishonchli aniqlash		●			●		●
Qurilmalarning tabiati real vaqtda kriminalistik yondashuvlarni qabul qilmasligi			●	●	●		
Dalillarni saqlash va ro‘yxatga olish bilan bog‘liq muammolar				●	●		
Turli ma’lumotlar manbalari tufayli dalil kontentlari ko‘payishi				●			
Ishonchning pastligi va saqlashning mustahkam zanjiri	●		●				
Qurilmalarda resurs cheklanganligi				●			

strategiyalarni, ma’lumotlar va saqlash tizimlarida qo‘llaniladigan shifrlash kabi kriminalistikaga qarama-qarshi usullarni, shuningdek, o‘ziga xos xavfsizlik choralariga ega mobil telefonlar va apparat bilan bog‘liq texnologik muammolarni o‘z ichiga oladi.

5. XULOSA

Kundalik hayotimizni raqamlashtirish ko‘p sonli afzallik va qulayliklardan tashqari, xavfsizlik muammolarini keltirib chiqaradi. Ushbu tadqiqot ishida raqamli ekspertizaning turli sohalaridagi asosiy muammolar keltirildi. Bundan tashqari, ushbu muammolarni vaqtga ko‘ra dolzarbligini ta’kidlash uchun yillar kesimida tahlil qilindi. Tadqiqot ishiga ko‘ra, raqamli ekspertizada tahlil bilan bir qatorda ma’lumotlarni

yig‘ish ko‘proq qiyinchiliklarni keltirib chiqaradigan bosqichdir. Agar kriminalistika sohasiga ko‘ra tahlil qilinsa, IoT da ko‘plab muammolar kuzatiladi, keyingi o‘rin esa multimedia va mobil qurilmalar raqamli ekspertizasiga tegishli. Boshqa sohalar singari, biznes sektorining davom etayotgan raqamlashtirishi kelgusi yillarda raqamli ekspertiza mexanizmlariga zarurat oshishini anglatadi. Shu sababli, bunday hollarda o‘rganilmagan muammolar yaqin kelajakda to‘siqlarga aylanishidan oldin faol tashabbuslarni talab qiladi. Mashinali o‘qitish va sun’iy intellekt asta-sekin ko‘plab vositalar va usullarning tarkibiga integratsiya qilinmoqda. Shunga qaramay, natijalarni tushunarli insoniy tarzda mulohaza qilish muammodir. Bundan tashqari, bulutli texnologiyalar, mobil qurilmalar, IoT, dronlar va boshqalar uchun raqamli kriminalistika jarayonlarini standartlashtirish ustuvor vazifaga aylanib bormoqda, chunki ular deyarli barcha zamonaviy raqamli ekspertizalarning ajralmas qismidir. Muammoga umumiy javob berish va bir xil choralarni qo‘llash kiberjinoyatlarga qarshi kurashda yuqori samara beradi.

ADABIYOTLAR

1. (2019). I. G. C. for Innovation. Global Guidelines for Digital Forensics Laboratories. The European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
2. C. Pasquini, I. Amerini, and G. Boato, ‘‘Media forensics on social media platforms: A survey,’’ EURASIP J. Inf. Secur., vol. 2021, no. 1, pp. 1–19, Dec. 2021.
3. K. Nance, H. Armstrong, and C. Armstrong, ‘‘Digital forensics: Defining an education agenda,’’ in Proc. 43rd Hawaii Int. Conf. Syst. Sci., 2010, pp. 1–10.
4. The European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
5. M. E. Alex and R. Kishore, ‘‘Forensics framework for cloud computing,’’ Comput. Elect. Eng., vol. 60, pp. 193–205, May 2017.
6. M. Khanafseh, M. Qatawneh, and W. Almobaideen, ‘‘A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics,’’ Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 8, pp. 610–629, 2019.
7. C. Patsakis, F. Casino, N. Lykousas, and V. Katos, ‘‘Unravelling Ariadne’s thread: Exploring the threats of decentralised DNS,’’ IEEE Access, vol. 8, pp. 118559–118571, 2020.

8. S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, ‘‘Network forensics: Review, taxonomy, and open challenges,’’ J. Netw. Comput. Appl., vol. 66, pp. 214–235, May 2016.
9. L. F. Sikos, ‘‘Packet analysis for network forensics: A comprehensive survey,’’ Forensic Sci. Int., Digit. Invest., vol. 32, Mar. 2020.
10. K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, ‘‘Current and future trends in mobile device forensics: A survey,’’ ACM Comput. Surv., vol. 51, no. 3, pp. 1–31, 2018.
11. K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, ‘‘A critical review of 7 years of mobile device forensics,’’ Digit. Invest., vol. 10, no. 4, pp. 323–349, Dec. 2013.
12. J. Hou, Y. Li, J. Yu, and W. Shi, ‘‘A survey on digital forensics in Internet of Things,’’ IEEE Internet Things J., vol. 7, no. 1, pp. 1–15, Jan. 2020.
13. A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, ‘‘The Internet of Things security: A survey encompassing unexplored areas and new insights,’’ Comput. Secur., vol. 112, Jan. 2022.
14. P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, and B. B. Bastaki, ‘‘The complexity of Internet of Things forensics: A state-of-the-art review,’’ Forensic Sci. Int., Digit. Invest., vol. 38, Sep. 2021.
15. A. Ross, S. Banerjee, and A. Chowdhury, ‘‘Security in smart cities: A brief review of digital forensic schemes for biometric data,’’ Pattern Recognit. Lett., vol. 138, pp. 346–354, Oct. 2020.
16. T. Latzo, R. Palutke, and F. Freiling, ‘‘A universal taxonomy and survey of forensic memory acquisition techniques,’’ Digit. Invest., vol. 28, pp. 56–69, Mar. 2019.
17. A. Case and G. G. Richard, ‘‘Memory forensics: The path forward,’’ Digit. Invest., vol. 20, pp. 23–33, Mar. 2017.
18. A. Al-Dhaqm, S. A. Razak, D. A. Dampier, K.-K. R. Choo, K. Siddique, R. A. Ikuesan, A. Alqarni, and V. R. Kebande, ‘‘Categorization and organization of database forensic investigation processes,’’ IEEE Access, vol. 8, pp. 112846–112858, 2020.
19. T. K. Dasaklis, F. Casino, and C. Patsakis, ‘‘Sok: Blockchain solutions for forensics,’’ in Technology Development for Security Practitioners. Cham, Switzerland: Springer, 2021.
20. M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, ‘‘Exploring the attack surface of blockchain: A comprehensive

survey,'' IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020.
21. M. Dalal and M. Juneja, ''Steganography and steganalysis (in digital forensics): A cybersecurity guide,'' Multimedia Tools Appl., vol. 80, no. 4, pp. 5723–5771, Feb. 2021.
22. E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, ''A survey of machine learning techniques in adversarial image forensics,'' Comput. Secur., vol. 100, Jan. 2021.
23. 136. S. Alharbi, J. Weber-Jahnke, and I. Traore, ''The proactive and reactive digital forensics investigation process: A systematic literature review,'' in Information Security and Assurance, T.-H. Kim, H. Adeli, R. J. Robles, and M. Balitanas, Eds. Berlin, Heidelberg: Springer, 2011, pp. 87–100.
24. A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, ''Research challenges and opportunities in drone forensics models,''Electronics, vol. 10, no. 13, p. 1519, Jun. 2021.
25. E. Mantas and C. Patsakis, ''Who watches the new watchmen? The challenges for drone digital forensics investigations,'' arXiv preprint arXiv:2021.12640, 2021.
26. Christa Miller. Career Paths In Digital Forensics: Practical Applications. Retrieved from https://articles.forensicfocus.com/2019/07/31/career-paths-in-digital-forensics-practical-applications/
27. Roussev, V. Digital forensic science: issues, methods, and challenges. Synthesis Lectures on Information Security, Privacy, & Trust. 2016.
28. C. Grajeda, F. Breitinger, and I. Baggili, ''Availability of datasets for digital forensics- and what is missing,'' Digit. Invest., vol. 22, pp. S94–S105, Aug. 2017. [Online].Available: https://www.sciencedirect.com/science/article/pii/S1742287617301913