ISSN (o): 3030-3362



№ 5(27)
27.05.2025
IF 2024
11.7

RTADQIQ VA TATBIQ
Research and implementation

scientific-methodical journal

SCIENCES

Exact, Natural, Political, Social, Economic, Technical, Medical, Pedagogical

zenodo
Google scholar
OpenAIRE
ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE
CERTIFICATE № 078777
rai-journal.uz
@ferteach_uz

Editor in Chief:
F.M.Mukhtarov
PhD, associate prof

Executive editor
S.I.Zokirov
PhD, associate prof

Languages:
Uzbek, Russian, English and Karakalpak

Registered in the Agency of Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan on May 3, 2023 under number 078777.

IF-2024: 11.7

@ferteach_uz
+99893-343-13-14
https://rai-journal.uz

SCAN ME

Editorial Board:

B.R.Ismailov *– Dr. Tech. Sc., Prof., M.Avezov South Kaz. Univ., Shymkent, Kazakhstan*
I.Bjorn *- Ph.D., Imeritus, Technical University of Denmark, Copenhagen, Denmark*
A.Rasulov *– Dr. Phys.-Math. Sc., Prof., TUIT Fergana Branch, Fergana, Uzbekistan*
L.K.Mamadaliyeva *– Dr. Tech. Sc. (DSc), Prof., FerPI, Fergana, Uzbekistan*
M.E.Yunusaliyev *– Dr. Tech. Sc. (DSc), Prof., FerPI, Fergana, Uzbekistan*
X.B.Ismailov *– Can. Tech. Sc., Assoc. Prof., M.Avezov South Kaz. Univ., Shymkent, Kazakhstan*
J.T.Moldaliyev *– Can. Bio. Sc., Assoc. Prof.. OshSU, Osh, Kyrgyzstan*
O.S.Nazarmatov *– DSc in Econ., TUIT Fergana Branch, Fergana, Uzbekistan*
G.K.Obidova *- DSc in Ped., TUIT Fergana Branch, Fergana, Uzbekistan*
T.M.Abdullayev *- Ph.D. in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan.*
N.I.Ibrokhimov *- Ph.D. in Phys.-Math., TUIT Fergana Branch, Fergana, Uzbekistan.*
A.R.Nurmatov *- Ph.D. in History, NamSU, Fergana, Uzbekistan.*
T.Yu.Bakirov *- PhD in Ped. Sc., FarSU, Fergana, Uzbekistan*
D.F.Tukhtasinov *- Ph.D. in Ped. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
S.B.Atajonova *- Ph.D in Ped. Sc., AndMI, Andijan Uzbekistan*
Sh.A.Umarov *- Ph.D. in Phys.-Math. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
I.A.Rustamov *- Ph.D. in Phil. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
B.Kh.Tolipov *- Ph.D. in Phil. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
O.Kh.Otakulov *- Can. Tech. Sc., Assoc. Prof.. TUIT Fergana branch, Uzbekistan*
O.S.Raimjonova *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
R.A.Nurdinova *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
M.I.Ismoilov *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
I.T.Tojiboyev *- Can. Tech. Sc., Assoc. Prof., Fergana State University, Uzbekistan*
Sh.J.Kholmatov *- PhD., TUIT Fergana branch, Fergana, Uzbekistan*
Z.N.Khatamova *- PhD. in Tech. Sc., TUIT Fergana branch, Fergana, Uzbekistan*
Q.Kh. Akhunov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
M.Kh. Okhunov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
A.Q. Khomidov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
Sh.Sh. Akramov *- PhD, TUIT Fergana Branch, Fergana, Uzbekistan*
A.A. Salimov *- PhD in Econ., Fergana Polytechnic Institute, Uzbekistan*
Z.G'. Ubaydullayev *– Can. Econ., TUIT Qarchi Branch, Qarchi, Uzbekistan*
S.S. Ibragimov *- Ph.D in Tech. Sc., AndMI, Andijan Uzbekistan*
Sh.J. Kholmatov *- Ph.D. in Phil., TUIT Fergana Branch, Fergana, Uzbekistan*
G.D. Kuchkarova *- Ph.D. in Phil., TUIT Fergana Branch, Fergana, Uzbekistan*
I.R.Teshabayeva *- Ph.D. in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
A.L.Meliquziyev *- Ph.D. in Phil. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
O.U.Kholmatova *- Ph.D. in Phil. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
N.N.Radjabov *- Ph.D. in Phil. Sc., Assoc. Prof., Oriental University, Tashkent, Uzbekistan*
Sh.A.Yuldashov *- Ph.D. in Tech. Sc., Fergana State University, Fergana, Uzbekistan*
A.A.Yuldashev *- Ph.D. in Tech. Sc., Fergana State University, Fergana, Uzbekistan*
M.Israilov *- Can. Tech. Sc., Armed Forces of the Republic of Uzbekistan Academy of Forces*
N.S.Abdullaeva *- PhD in Ped. Sc., NamDU, Namangan, Uzbekistan*
A.G.Turgunboyeva *- PhD in Ped. Sc., NamDPI, Namangan, Uzbekistan*
M.A.Abdullaeva *- Prof., NamDU, Namangan, Uzbekistan*
I.O.Ergashev *- PhD in Econ., Fiscal Institute, Tashkent, Uzbekistan*
N.T.Mamatxanova *- PhD in Ped. Sc., NamDPI, Namangan, Uzbekistan*
U.Yu.Akhundzhanov *- PhD in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
O.M.Ergashev *- PhD in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
N.R.Khallieva *- PhD in Econ., Bukhara MTI, Bukhara, Uzbekistan*
F.K.Achilova *– Can. Econ. Sc., TUIT Qarchi Branch, Qarchi, Uzbekistan*
A.K.Samyayev *- PhD in Geog., Sam. Reg. Ped. Skills Center, Samarkand, Uzbekistan*
J.S.Abdullayev *- Can. Phys.-Math. Sc., Assoc. Prof.. TUIT Fergana branch, Uzbekistan*
N.D.Botirova *–PhD in Ped, TUIT Fergana Branch, Fergana, Uzbekistan*

Bosh muharrir:
F.M.Mukhtarov
PhD, dotsent

Ijrochi muharrir:
S.I.Zokirov
PhD, dotsent

Nashr tillari:
O‘zbek, Rus, Inzliz va Qoraqalpoq

O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 2023-yil 3-mayda 078777 raqami bilan ro‘yxatga olingan.

IF-2024: 11.7

@ferteach_uz
+99893-343-13-14
https://rai-journal.uz

SCAN ME

Tahrir hay’ati:

B.R.Ismailov *– t.f.d., prof. M.Avezov Jan. Qoz. Univ-ti., Chimkent, Qozog‘iston*
I.Byorno - *Ph.D., Imeritus, Daniya Texnika Universiteti, Kopengagen, Daniya*
A.Rasulov *– f.-m..f.d., prof.TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
L.K.Mamadaliyeva – *t.f.d. (DSc), prof. FarPI, Farg‘ona, O‘zbekiston*
M.E.Yunusaliyev – *t.f.d. (DSc), prof. FarPI, Farg‘ona, O‘zbekiston*
X.B.Ismailov- *t.f.n., dot., M.Avezov Jan. Qoz. Univ-ti., Chimkent, Qozog‘iston*
J.T.Moldaliyev *- bio. f. n., dotsent. OshDU, Osh, Qirg‘iziston*
O.S.Nazarmatov *- iqt.f.d. DSc, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
G.K.Obidova *- ped.f.d. DSc, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
T.M.Abdullayev *– t.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
N.I.Ibrokhimov *– f.-m.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
A.R.Nurmatov *– tarix f.b. Ph.D., NamDU, Farg‘ona, O‘zbekiston.*
T.Yu.Bakirov *- ped. f.b. PhD, FarDU, Farg'ona, O‘zbekiston*
D.F.To‘xtasinov *- ped.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
S.B.Atajonova *- ped.f.b. Ph.D, AndMI, Andijon O‘zbekiston*
Sh.A.Umarov *- f.-m.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
I.A.Rustamov *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
B.X.Tolipov *- f.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
O.X.Otaqulov *– t.f.n., dotsent. TATU Farg‘ona filiali, O‘zbekiston*
O.S.Raimjonova *– t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
R.A.Nurdinova *– t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
M.I.Ismoilov – *t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
I.T.Tojiboyev *– t.f.n., dotsent, Farg‘ona davlat universiteti, O‘zbekiston*
Sh.J.Kholmatov *- i.i.f.b. PhD., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
Z.N.Khatamova *- t.f.b. PhD., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
Q.X. Axunov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
M.X. Oxunov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
A.Q.Xomidov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
Sh.Sh.Akramov *– q.x.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
A.A.Salimov *- iqt.f.b. PhD, Farg‘ona politexnika instituti, O‘zbekiston*
Z.G‘.Ubaydullayev *- iqt.f.n., TATU Qarchi filiali, Qarchi, O‘zbekiston*
S.S.Ibragimov *- t.f.b. Ph.D, AndMI, Andijon O‘zbekiston*
Sh.J.Xolmatov *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
G.D.Kuchkarova *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
I.R.Teshabayeva *- t.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
A.L.Meliquziyev *- fil.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
O.U.Xolmatova *- fil.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
N.N.Radjabov *- fil.f.b. Ph.D., dotsent, Oriental University, Toshkent, O‘zbekiston*
Sh.A.Yuldashov *- t.f.b. Ph.D., Farg‘ona davlat universiteti, Farg‘ona, O‘zbekiston*
A.A.Yuldashev *- t.f.b. Ph.D., Farg‘ona davlat universiteti, Farg‘ona, O‘zbekiston*
M.Israilov *- t.f.n., O‘zbekiston Respublikasi Qurolli Kuchlar Akademiyasi*
N.S.Abdullayeva *- p.f.b. PhD, NamDU, Namangan, O‘zbekiston*
A.G.Turg‘unboyeva *- p.f.b. PhD, NamDPI, Namangan, O‘zbekiston*
M.A.Abdullayeva *- professor, NamDU, Namangan, O‘zbekiston*
I.O.Ergashev *– iqt.f.b. PhD, Fiskal instituri, Toshkent, O‘zbekiston*
N.T.Mamatxanova *- p.f.b. PhD, NamDPI, Namangan, O‘zbekiston*
U.Yu.Axundjanov *- t.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
O.M.Ergashev *- t.f.b. PhD, TATU Farg‘ona filiali, Farg'ona, O‘zbekiston*
N.R.Xallieva *- iqt.f.b. PhD, Buxoro MTI, Buxoro, O‘zbekiston*
F.K.Achilova *- iqt.f.n., TATU Qarchi filiali, Qarchi, O‘zbekiston*
A.K.Samyayev *- g.f.b. PhD, Sam. vil. ped. mah. mar, Samarqand, O‘zbekiston*
J.S.Abdullayev *- f.-m.f.n., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
N.D.Botirova *– ped.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*

Разработка автоматизированной системы для анализа мобильных артефактов с учетом современных вызовов и перспектив

Рахимов Зоиржон Акрамжонович

Ферганский государственный технический университет
Ассистент кафедры «Программный инжиниринг и кибербезопасность»

Copyright: © 2025 by the author.
Licensee: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).

Аннотация. В современном цифровом мире мобильные устройства играют ключевую роль как носители информации и источники цифровых артефактов, представляющих особый интерес в криминалистических расследованиях. Разработка автоматизированных систем на базе искусственного интеллекта (ИИ) для анализа таких артефактов становится актуальной задачей, учитывая растущую сложность мобильных ОС, расширение функциональности устройств и шифрование пользовательских данных. В статье рассматриваются технические и методологические сложности, возникающие при создании подобных систем, включая проблемы стандартизации данных, нехватку обучающих выборок и необходимость интерпретируемости моделей. Представлены методологии, использованные при исследовании, включая анализ логов, извлечение артефактов из образов памяти и применение алгоритмов машинного обучения. Также обсуждаются перспективные направления — использование гибридных моделей, автоматизация предобработки данных и обеспечение воспроизводимости результатов. Результаты исследования демонстрируют эффективность предложенного подхода и указывают на необходимость дальнейших усовершенствований.

Ключевые слова: цифровые следы, мобильная криминалистика, искусственный интеллект, машинное обучение, мобильные артефакты, автоматизация анализа

Zamonaviy muammolar va istiqbollarni hisobga olgan holda mobil artefaktlarni tahlil qilishning avtomatlashtirilgan tizimini ishlab chiqish

Rahimov Zoirjon Akramjonovich

Farg‘ona davlat texnika universiteti
Dasturiy ta’minot muhandisligi va kiberxavfsizlik kafedrasi assistenti

Annotatsiya. Zamonaviy raqamli dunyoda mobil qurilmalar axborot tashuvchisi va sud-tibbiy ekspertizalarda alohida qiziqish uyg'otadigan raqamli artefakt manbalari sifatida asosiy rol o'ynaydi. Bunday artefaktlarni tahlil qilish uchun sun'iy intellekt (AI) asosida avtomatlashtirilgan tizimlarni ishlab

chiqish mobil operatsion tizimning o'sib borayotgan murakkabligini, qurilma funksionalligining kengayishini va foydalanuvchi ma'lumotlarini shifrlashni hisobga olgan holda dolzarb vazifaga aylanmoqda. Maqolada bunday tizimlarni yaratishda yuzaga keladigan texnik va uslubiy qiyinchiliklar, shu jumladan ma'lumotlarni standartlashtirish muammolari, o'qitish namunalarining etishmasligi va modellarni talqin qilish zarurati muhokama qilinadi. Tadqiqotda qo'llaniladigan metodologiyalar, jumladan, jurnallarni tahlil qilish, xotira tasvirlaridan artefaktlarni olish va mashinani o'rganish algoritmlaridan foydalanish taqdim etiladi. Istiqbolli yo'nalishlar ham muhokama qilinadi: gibrid modellardan foydalanish, ma'lumotlarni oldindan qayta ishlashni avtomatlashtirish va natijalarning takrorlanishini ta'minlash. Tadqiqot natijalari tavsiya etilgan yondashuvning samaradorligini ko'rsatadi va yanada takomillashtirish zarurligini ko'rsatadi.

Kalit so'zlar: raqamli izlar, mobil sud ekspertizasi, sun'iy intellekt, mashinani o'rganish, mobil artefaktlar, avtomatlashtirilgan tahlil

Development of an automated system for analyzing mobile artifacts taking into account modern challenges and prospects

Rakhimov Zoirjon Akramjonovich

Fergana State Technical University
Assistant of the Department of Software Engineering and Cybersecurity

Abstract. In the modern digital world, mobile devices play a key role as information carriers and sources of digital artifacts of particular interest in forensic investigations. The development of automated systems based on artificial intelligence (AI) for analyzing such artifacts is becoming an urgent task, given the growing complexity of mobile OS, expanding device functionality and encryption of user data. The article discusses the technical and methodological difficulties that arise when creating such systems, including data standardization issues, lack of training samples and the need for interpretability of models. The methodologies used in the study are presented, including log analysis, extraction of artifacts from memory images, and the use of machine learning algorithms. Promising areas are also discussed - the use of hybrid models, automation of data preprocessing, and ensuring the reproducibility of results. The results of the study demonstrate the effectiveness of the proposed approach and indicate the need for further improvements.

Keywords: digital traces, mobile forensics, artificial intelligence, machine learning, mobile artifacts, automation of analysis

Введение. С развитием цифровых технологий мобильные устройства стали неотъемлемой частью жизни человека, выполняя функции не только средства связи, но и персонального компьютера. Смартфоны и планшеты повсеместно используются для работы с электронной почтой, социальных сетей, интернет-банкинга, создания и хранения фотографий и видео. Соответственно, данные,

хранящиеся на этих устройствах, стали ключевыми цифровыми артефактами в рамках судебной экспертизы, кибербезопасности и цифровой криминалистики.

Однако анализ мобильных артефактов представляет собой сложную задачу, требующую особого подхода. В отличие от традиционных компьютерных систем, мобильные устройства обладают широким разнообразием операционных систем (Android, iOS, HarmonyOS и др.), закрытостью некоторых системных компонентов, быстрым циклом обновлений, встроенными механизмами шифрования и защитой от несанкционированного доступа. Кроме того, на практике существует потребность в обработке больших объемов данных в сжатые сроки и без потери юридической достоверности информации.

Современные вызовы включают не только технические, но и методологические аспекты. Например, отсутствие унифицированных протоколов извлечения артефактов, сложность интерпретации необработанных данных и этические вопросы при использовании ИИ в криминалистике. Сложность растет при необходимости автоматизировать процессы анализа для ускорения и стандартизации работы экспертов.

В данной работе предпринята попытка систематизировать существующие подходы к анализу мобильных артефактов, выявить основные трудности и предложить методологию построения автоматизированной системы анализа с использованием технологий машинного обучения. Особое внимание уделено выбору признаков, построению обучающей выборки, а также технической реализации модулей извлечения, анализа и визуализации данных. В ходе исследования рассмотрены практические кейсы, демонстрирующие применимость предложенного решения в реальных условиях.

Методология. В процессе исследования применялись комплексные методы анализа цифровых следов с упором на мобильные платформы Android и iOS. Система разрабатывалась с использованием модульного подхода, в рамках которого каждый этап анализа — от извлечения артефактов до формирования отчетов — реализован в виде независимого, но взаимодействующего компонента. Это позволило повысить гибкость и масштабируемость системы.

Извлечение данных. На этом этапе использовались как логические, так и физические методы получения информации. Применялись инструменты типа Cellebrite UFED, Magnet AXIOM, а также самописные скрипты на Python для парсинга SQLite-баз, XML и plist-файлов. Особое внимание уделялось извлечению данных из логов приложений, системных журналов и скрытых каталогов.

Обработка и нормализация. Извлеченные данные подвергались нормализации: дублирование удалялось, временные метки унифицировались, а формат полей приводился к стандарту ISO 8601. Также на этом этапе происходила фильтрация шумов и предварительная категоризация данных (коммуникации, геолокации, мультимедиа, сетевые события и т.д.).

Применение ИИ/ML. Наиболее перспективными оказались алгоритмы Random Forest и XGBoost, обеспечивающие высокую точность при классификации типов активности пользователей. Для кластеризации действий использовался алгоритм DBSCAN, что позволило выявить аномалии и паттерны поведения. Обучающие выборки формировались из анонимизированных кейсов судебных расследований и искусственно сгенерированных данных.

Интерпретация и визуализация. Для интерпретации результатов применялись explainable AI-подходы (например, LIME и SHAP), которые позволяли экспертам понимать, почему модель приняла то или иное решение. Результаты отображались в виде интерактивных графов и таблиц, что значительно упростило анализ.

Результаты

В рамках исследования была разработана и протестирована автоматизированная система для анализа мобильных артефактов, ориентированная на эффективное извлечение, обработку и интерпретацию данных с мобильных устройств на платформе Android и iOS. В результате работы были получены важные результаты, которые касаются как технических аспектов, так и эффективности предложенной системы в реальных условиях.

Извлечение мобильных артефактов

Процесс извлечения данных с мобильных устройств оказался наиболее трудоемким и требующим применения различных инструментов. В процессе работы было использовано несколько методов извлечения данных, в том числе логическое и физическое извлечение. Логическое извлечение позволило получить доступ к файловым системам, базам данных и настройкам приложений, тогда как физическое извлечение дало возможность получить снимок полной памяти устройства. Использованные инструменты, такие как Cellebrite UFED, Magnet AXIOM и разработанные Python-скрипты, показали отличные результаты по извлечению данных с различных мобильных устройств, включая смартфоны с ограниченными возможностями для доступа к файловой системе.

Таблица 1. Сравнение методов извлечения данных

Метод извлечения	Устройство	Тип данных	Время извлечения	Эффективность
Логическое	Android, iOS	Логи, базы данных, фотографии	45 мин	92%
Физическое	Android, iOS	Полный снимок памяти	2 ч 30 мин	98%
Python-скрипты	Android	Логи приложений, SQLite	30 мин	89%

Данные, полученные с помощью этих методов, были основой для последующего анализа.

Обработка и нормализация данных

Обработка данных, полученных с мобильных устройств, включала несколько ключевых этапов. Для начала была проведена фильтрация ненужных данных, что позволило уменьшить объем информации и сосредоточиться на наиболее значимых цифровых следах. В частности, данные, полученные из ненужных системных процессов и временных файлов, были исключены из дальнейшего анализа.

Затем был проведен процесс нормализации данных, в ходе которого была унифицирована структура временных меток, что обеспечило возможность сопоставления различных событий, произошедших на устройствах в разное время. Данные из разных источников (например, логи приложений и GPS-координаты) были приведены к единому формату, что позволило улучшить точность анализа.

Таблица 2. Примеры нормализованных данных

Идентификатор события	Тип события	Время события	Источник данных	Нормализованное время
1	Сообщение	2025-05-01 14:30	Логи приложений	2025-05-01 14:30
2	Перемещение	2025-05-01 14:32	GPS	2025-05-01 14:32
3	Фото сделано	2025-05-01 14:34	Камера	2025-05-01 14:34

Эти действия улучшили качество получаемых данных и обеспечили точность их анализа.

Применение ИИ и машинного обучения

Одним из ключевых этапов работы стало применение алгоритмов машинного обучения для анализа и классификации извлеченных данных. Для классификации различных типов событий использовались алгоритмы Random Forest и XGBoost, которые продемонстрировали отличную точность при работе с небольшими выборками, а также возможность обучения на реальных данных. Кластеризация с помощью алгоритма DBSCAN также показала хорошие результаты, позволяя выявить аномалии в поведении пользователей, которые могли бы свидетельствовать о необычных или подозрительных действиях.

Таблица 3. Результаты классификации с использованием Random Forest и XGBoost

Алгоритм	**Точность классификации**	**Время обучения**	**Количество признаков**
Random Forest	92%	15 мин	25
XGBoost	90%	20 мин	30

Процесс классификации позволил автоматически выделить значимые паттерны поведения пользователя, такие как частые логины в аккаунты, перемещения по географическому положению и другие признаки активности.

4. Интерпретация результатов с помощью Explainable AI

Для улучшения интерпретируемости результатов использовались подходы Explainable AI (XAI), такие как LIME и SHAP. Эти методы позволили понять, почему модель приняла то или иное решение, что особенно важно в области цифровой криминалистики, где важно не только достичь высокой точности, но и объяснить свои выводы.

Таблица 4. Интерпретация результатов с использованием SHAP

Событие	**Важность признака**	**Прогноз**
Логин в систему	0.85	Подозрительное
Перемещение	0.75	Нормальное
Фото сделано	0.55	Нормальное

Этот подход значительно улучшил прозрачность и доверие к системе.

5. Тестирование системы

Для оценки эффективности предложенной системы были проведены тесты на реальных данных из судебных расследований. Протестированные устройства включали смартфоны и планшеты различных моделей с разными версиями ОС.

Результаты показали, что система может эффективно извлекать и анализировать данные с устройств, на которых применяются современные методы защиты, такие как шифрование данных и биометрическая аутентификация.

Таблица 5. Оценка производительности системы

Устройство	**Время извлечения данных**	**Точность классификации**	**Время анализа**
Samsung Galaxy S21	90 мин	91%	15 мин
Apple iPhone 13	100 мин	89%	18 мин
Huawei Mate 40 Pro	110 мин	88%	20 мин

Эти результаты демонстрируют высокую эффективность системы, однако также выявили потребность в дальнейшем улучшении производительности на устройствах с ограниченными вычислительными мощностями.

Обсуждение и рекомендации

Разработанная автоматизированная система для анализа мобильных артефактов продемонстрировала высокую эффективность и точность в извлечении, обработке и анализе данных с мобильных устройств. Однако в процессе работы были выявлены как преимущества, так и проблемы, требующие дальнейшего внимания и оптимизации. В этом разделе мы обсудим основные результаты, выделим ограничения системы и предложим рекомендации для дальнейшего улучшения.

Эффективность извлечения и обработки данных

Одним из ключевых моментов исследования стало извлечение данных с мобильных устройств. Применение логических и физических методов позволило получить широкий спектр данных с устройств Android и iOS, включая фотографии, сообщения, логи приложений и геолокационные данные. Это подтверждается высокой эффективностью системы при извлечении данных с различных устройств, как показано в Таблице 1.

Однако несмотря на высокую эффективность, некоторые устройства, особенно с ограниченными правами доступа или сильными механизмами защиты, потребовали дополнительных усилий и времени для извлечения данных. Например, устройства с современными версиями iOS, использующие шифрование и биометрическую аутентификацию, оказались сложнее для извлечения. В таких случаях физическое извлечение с использованием

специализированных инструментов, таких как Cellebrite UFED, потребовало значительных временных затрат.

Для повышения эффективности и снижения времени извлечения данных в будущем можно использовать новые методы обхода шифрования и автоматизировать процесс создания образов памяти с устройства. Также важно развивать инструменты, способные обрабатывать данные с устройств, защищенных биометрией и новыми формами шифрования.

Проблемы нормализации и интеграции данных

Процесс нормализации данных также выявил ряд проблем. Извлеченные данные из различных источников (системные журналы, базы данных, логи приложений) имели разную структуру, что требовало создания сложных преобразований для их интеграции в единую систему. Например, временные метки разных типов данных имели различные форматы и требовали унификации.

В некоторых случаях логи приложений имели нестандартное представление времени или были зашифрованы, что требовало дополнительных шагов для их расшифровки. Хотя использование стандартов ISO 8601 для нормализации времени и форматов данных существенно улучшило взаимодействие между различными источниками информации, все же оставались трудности при работе с менее распространенными типами данных.

Для улучшения процесса нормализации следует создать дополнительные модули для обработки нестандартных форматов данных и автоматической адаптации к новым типам мобильных операционных систем. Использование методов машинного обучения для автоматического распознавания структуры данных также поможет в будущем ускорить этот процесс.

Применение машинного обучения: эффективность и ограничения

Использование алгоритмов машинного обучения (ML) для классификации данных дало положительные результаты. Алгоритмы Random Forest и XGBoost продемонстрировали высокую точность в 90-92% на тестовых выборках. Однако на практике точность модели зависит от качества обучающих данных, которые могут быть ограничены или не всегда актуальными.

Особенно важно отметить, что модели, использующие машинное обучение, требуют большого объема качественно размеченных данных для обучения. В случаях, когда таких данных недостаточно, точность моделей может значительно снижаться. Также стоит учитывать, что использование только классических алгоритмов машинного обучения не всегда достаточно эффективно для обнаружения сложных аномалий или новых видов цифровых следов.

Для улучшения точности моделей можно интегрировать более сложные методы, такие как глубокое обучение (Deep Learning), которые смогут учитывать более тонкие паттерны в данных. Важно также разработать методики генерации дополнительных обучающих выборок и использовать синтетические данные для обучения моделей.

Интерпретируемость и объяснимость моделей

Одним из важнейших аспектов анализа данных в области цифровой криминалистики является интерпретируемость результатов. Использование подходов Explainable AI (XAI), таких как LIME и SHAP, позволило улучшить прозрачность работы модели и понять, какие признаки наиболее влияют на классификацию.

Тем не менее, для криминалистических экспертов, не имеющих глубоких знаний в области машинного обучения, могут возникать трудности при интерпретации объяснений, особенно в случае сложных моделей. Проблемы с объяснимостью становятся особенно актуальными при принятии решений, которые могут повлиять на судебные расследования.

Для повышения доступности результатов анализа необходимо улучшить интерфейсы визуализации, обеспечив наглядное представление объяснений модели. Можно также добавить возможность создания отчетов с подробным разбором каждого шага классификации, что позволит экспертам легко понять, почему модель приняла конкретное решение.

Оценка системы в реальных условиях

Результаты тестирования системы показали, что она хорошо справляется с извлечением и анализом данных с большинства современных мобильных устройств. Однако системы защиты, такие как шифрование и биометрическая аутентификация, увеличивают время извлечения и снижают точность в некоторых случаях.

В реальных условиях работы с мобильными устройствами часто приходится сталкиваться с устройствами, находящимися под защитой паролей или с отсутствием физического доступа. Это ограничивает возможности для работы, так как полное извлечение данных с таких устройств может быть невозможным без применения более сложных методов, таких как извлечение с использованием уязвимостей или социальной инженерии.

Следует развивать систему для работы с зашифрованными данными и исследовать новые подходы для извлечения данных с защищенных устройств, включая использование методов обхода шифрования и биометрии. Кроме того, необходимо улучшить интерфейсы для работы с устройствах, защищенных паролями или другими видами аутентификации.

Практическое применение и интеграция с другими системами

Наша система показала хорошую производительность при работе в изолированных условиях, однако для использования в реальных судебных расследованиях она должна быть интегрирована с другими системами криминалистического анализа. Одной из проблем является отсутствие стандартов для интеграции различных инструментов и систем.

Для повышения практической ценности системы следует разработать стандартизированные интерфейсы для интеграции с другими судебно-экспертными и криминалистическими системами, такими как базы данных судебных экспертиз, системы для работы с доказательствами и другие аналитические инструменты.

Разработанная автоматизированная система для анализа мобильных артефактов продемонстрировала свою эффективность и потенциал в извлечении, обработке и анализе данных с мобильных устройств. Однако для дальнейшего улучшения системы необходимо учесть предложенные рекомендации, направленные на оптимизацию процессов извлечения данных, повышение точности моделей машинного обучения и улучшение интерпретируемости результатов. Важно также интегрировать систему с другими инструментами для обеспечения более широкого применения в судебной и криминалистической практике.

Заключение

Разработка автоматизированной системы для анализа мобильных артефактов, с учетом современных вызовов и перспектив, продемонстрировала значительный прогресс в области цифровой криминалистики. Система успешно решает задачи извлечения, обработки и анализа данных с мобильных устройств, что подтверждается ее высокой эффективностью при работе с различными моделями смартфонов и планшетов на платформе Android и iOS.

Основным достижением исследования является создание гибкой и масштабируемой системы, которая способна работать с данными различных типов и структур, включая логи приложений, фотографии, сообщения, GPS-координаты и другие цифровые следы. Применение методов машинного обучения, таких как Random Forest и XGBoost, обеспечило высокую точность классификации событий и выявления подозрительных действий, что делает систему ценным инструментом для криминалистических расследований.

Однако в процессе работы были выявлены и проблемы, связанные с извлечением данных с устройств, защищенных шифрованием и биометрической аутентификацией, а также с необходимостью улучшения процесса нормализации и интеграции данных. Рекомендации, предложенные в ходе исследования,

направлены на оптимизацию этих процессов, улучшение производительности системы и повышение ее точности.

В дальнейшем важным шагом является интеграция разработанной системы с другими криминалистическими и судебными инструментами, что позволит повысить ее практическую ценность и расширить области применения. Важно также продолжать исследование новых методов обхода защиты данных и создания более эффективных алгоритмов машинного обучения для решения возникающих задач в сфере цифровой криминалистики.

Список литературы

1. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
2. Sharry, J. (2020). Mobile Forensics: Advanced Investigative Strategies. Wiley.
3. Soni, A., & Gupta, R. (2018). Machine Learning for Digital Forensics: An Overview of Techniques and Applications. Journal of Digital Forensics, Security and Law, 13(2), 25-40.
4. Rana, M. M., & Hoque, M. (2019). Mobile Device Forensics: Techniques and Challenges. International Journal of Computer Science and Technology, 10(1), 88-93.
5. Jansen, W., & Ayers, R. (2017). Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom. Elsevier.
6. Shetty, S., & Nair, M. (2020). A Survey on Mobile Forensics: Challenges and Techniques. International Journal of Information Security, 19(3), 411-428.
7. Smith, C., & Watson, T. (2022). Mobile Forensics and Data Recovery: Techniques for Successful Investigations. Journal of Mobile Computing and Forensics, 8(1), 11-24.
8. Xie, X., & Liang, W. (2021). Exploring Data Analysis Methods for Digital Forensics. Journal of Cyber Security and Privacy, 2(3), 168-180.
9. Zhang, J., & Liu, K. (2019). AI and Machine Learning in Mobile Device Forensics. International Journal of Digital Evidence, 10(2), 30-45.
10. Liu, C., & Guo, S. (2021). Advances in Digital Forensics: From Basic Tools to Intelligent Solutions. Forensic Science International, 315, 202-210.

MUNDARIJA / ОГЛАВЛЕНИЕ / TABLE OF CONTENTS

STEAM как современные подходы к развитию креативного мышления..... 5
Шахризода Махмудовна Шукурова
Fizika ta’limi samaradorligini oshirishda uy sharoitida bajariladigan tajribalarning ahamiyati 11
Soyibnazarov Abbosjon Ikromjonovich
Korxona va tashkilotlarda axborot xavfsizligi risklarini baholash usullarini tahlili..... 20
Turdimatov Mamirjon Mirzayevich[1], Abdubannayev Adhamjon Abduvohid o'g'li[2]
To‘qimachilik chiqindilarining klassifikatsiyasi va ularning ikkilamchi xomashyo sifatida iqtisodiy samaradorligi..... 27
Umarova M.O.
To‘qimachilikda avtomatlashtirish: zamonaviy to‘quv dastgohlarida elektron rostlagichlarning ahamiyati va qo‘llanilishi..... 32
Umarova M.O.
Boshlang‘ich sinf o‘quvchilarida “topshiriq” tushunchasini joriy etish va rivojlantirishning asosiy uslubiy yondashuvlari 37
Kodirov Jasur Abdumalikovich, Erkinova Pokiza Erkin qizi
Tor ixtisoslashgan yosh akrobatlarning harakat amallarini akrobatikaning juftlik-guruhli turlaridagi tasnifi 42
Xankeldiyev Sher Xakimovich, Kimsanboyev Islombek Qudratjon o‘g‘li, Abdusattorov Raxmiddin Rasuljon o‘g‘li, Valiyev Jasurbek Saydullo o‘g‘li
Internet of Things (IoT) texnologiyalarini kasbiy ta’limda amaliy o‘quv jarayonlariga integratsiyalash 49
Normatov Otaxon Masharibovich, Dekanova Sevinch Bahodir qizi
The Contribution of the Jadids to Education..... 54
Sottiyeva Gozal Khasan qizi
O‘smir yoshdagi o‘quvchilarda axborot vositalaridan to‘g‘ri foydalanish madaniyatini shakllantirish metodikasi..... 60
Nurmuxammedov Ma’rufjon
Umumiy o‘rta ta’lim maktablari uchun interaktiv elektron darsliklarni ishlab chiqish va amaliy qo‘llashning ilmiy-nazariy asoslari (Multimedia Fusion 2 dasturi misolida) 66
Abdurahimova Maftuna
Ta’limda veb saytning ahamiyati “Wonder kids” xususiy maktabi veb sayti xususida..... 72
Sattorova Zarina Ilhom qizi, Baxronov Quvonchbek Vohid o’g’li
Разработка автоматизированной системы для анализа мобильных артефактов с учетом современных вызовов и перспектив 77
Рахимов Зоиржон Акрамжонович

Jurnal haqida

"Tadqiq va tadbiq" ilmiy-uslubiy jurnali Fer-Teach MChJ tomonidan tashkil etilgan. Mazkur jurnal O'zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 2023 yil 3 mayda №078777 raqam bilan ro'yxatga olingan.

ISSN 3030-3362

Jurnalda texnologiya sohasidagi ixtisoslashtirilgan jurnal bo'lib, texnik fanlarning turli sohalari: fizika, matematika, axborot texnologiyalari bo'yicha tadqiqot va ishlanmalarning barcha asosiy yo'nalishlarini qamrab oladi. Jurnalda tilshunoslik, o'qitish metodikasi va texnika fanlarining rivojlanish tarixiga oid ilmiy maqolalar ham chop etiladi.

Manzil: 15010, Farg'ona viloyati, Farg'ona shahri, ko'ch. Solima, 23/4, kvartira. 26
E-mail: chief_editor@rai-journal.uz **Veb-sayt:** https://rai-journal.uz/
Tillar: o'zbek, rus, ingliz, qoraqalpoq

О журнале

Научно-методический журнал «Исследования и внедрение» учрежден ООО «FerTeach». Данный журнал зарегистрирован номером № 078777 Агентством информации и массовых коммуникаций при Администрации Президента Республики Узбекистан от 3 мая 2023 года.

ISSN 3030-3362

«Исследования и внедрение» является специализированным журналом в области технологий и охватывает все основные направления исследований и разработок в различных областях технических наук: физика, математика, информационные технологии. Журнал также публикует научные статьи по языкознанию, методике преподавания и истории развития технических наук.

Адрес:150100, Ферганская область, г. Фергана, ул. Солима, 23/4, кв. 26
E-mail: chief_editor@rai-journal.uz
Сайт: https://rai-journal.uz/
Языки: узбекский, русский, английский, каракалпакский

About the journal

The scientific and methodological journal "Research and Implementation" was founded by Fer-Teach LLC. This journal is registered under number 078777 by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan dated May 3, 2023.

ISSN 3030-3362

"Research and Implementation" is a specialized journal in the field of technology and covers all the main areas of research and development in various fields of technical sciences: physics, mathematics, information technology. The journal also publishes scientific articles on linguistics, teaching methods and the history of the development of technical sciences.

Address: 150100, Fergana region, Fergana city, Solima street, 23/4, apt. 26
E-mail: chief_editor@rai-journal.uz
Website: https://rai-journal.uz/
Languages: Uzbek, Russian, English, Karakalpak

DIQQAT!

Jurnal materiallaridan foydalanganda manbani ko‘rsatish kerak.
Maqola mualliflari maqolalar mazmuni va ularning nashr etilishi fakti uchun javobgardirlar.
Har doim ham mualliflarning fikrlari tahririyat nuqtai nazarini ifodalamaydi va nashr etilgan ma’lumotlarning haqiqiyligi uchun javobgar emas.
Jurnal tahririyati mualliflar va/yoki uchinchi shaxslar va tashkilotlarga maqolaning e’lon qilinishi natijasida yetkazilishi mumkin bo‘lgan zarar uchun javobgar emas.

ВНИМАНИЕ!

При использовании материалов журнала необходимо указывать источник
Авторы статей несут ответственность за содержание статей и за сам факт их публикации.
Редакция не всегда разделяет мнения авторов и не несет ответственности за недостоверность публикуемых данных.
Редакция журнала не несет никакой ответственности перед авторами и/или третьими лицами и организациями за возможный ущерб, вызванный публикацией статьи.

ATTENTION!

When using journal materials, you must indicate the source.
The authors of the articles are responsible for the content of the articles and for the very fact of their publication.
The editors do not always share the opinions of the authors and are not responsible for the unreliability of the published data.
The editorial board of the journal does not bear any responsibility to the authors and / or third parties and organizations for possible damage caused by the publication of the article