



LARANA, INC.

# **IOS 13 ОПЕРАЦИЯЛЫҚ ЖҮЙЕСІНДЕГІ СОТ САРАПТАМАСЫНЫҢ ӘДІСТЕРІ МЕН ТЕХНОЛОГИЯЛАРЫ**

**БЕКБОЛАТОВА ДИАНА АҚЖ-35**

# МАЗМҰНЫ

01

КРИМИНАЛИСТИКАҒА КІРІСПЕ

02

САНДЫҚ ОРТАДАҒЫ СОТ САРАПТАМАСЫНЫҢ МАҢЫЗЫ

03

ЦИФРЛЫҚ ІЗДЕРДІ ТАЛДАУДАҒЫ IOS 13 ОПЕРАЦИЯЛЫҚ ЖҮЙЕСІНІҢ  
РӨЛІ

04

IOS 13 ҚҰРЫЛҒЫЛАРЫНАН ДЕРЕКТЕРДІ ШЫҒАРУҒА АРНАЛҒАН ҚҰРАЛДАР

05

ФИЗИКАЛЫҚ ЖӘНЕ ЛОГИКАЛЫҚ МӘЛІМЕТТЕРДІ АЛУ ӘДІСТЕРІ

06

IOS 13 ФАЙЛДЫҚ ЖҮЙЕСІН ТАЛДАУ

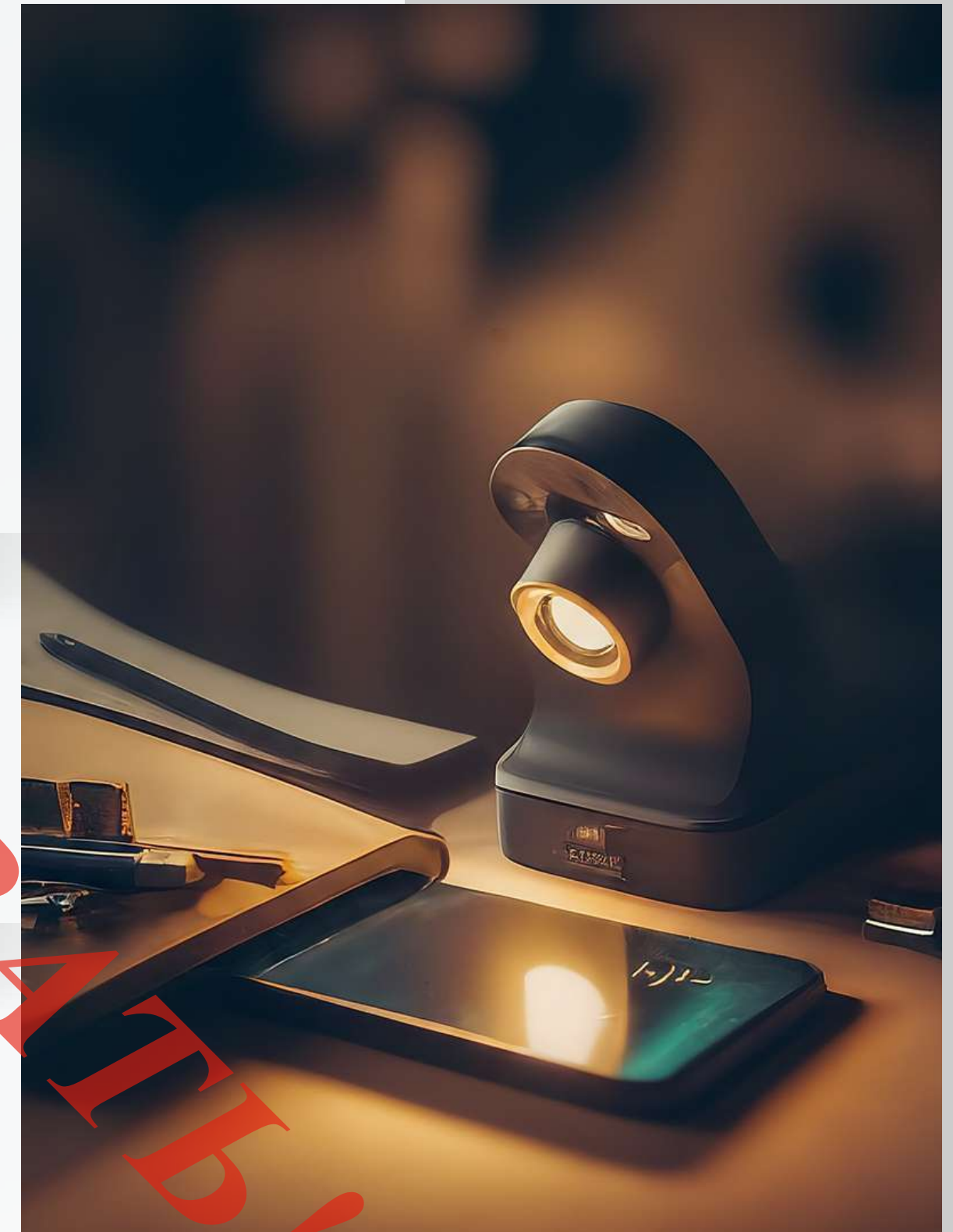
07

МЕТАДЕРЕКТЕРДІ ТАЛДАУ

# КРИМИНАЛИСТИКАҒА КІРІСПЕ



Сот сараптамасы қазіргі әлемнің ажырамас бөлігіне айналды, әсіресе электронды түрде көбірек деректер мен дәлелдемелер сақталатын цифрлық ғасырда. Әлемдегі ең танымалдардың бірі болып табылатын Apple компаниясының iOS 13 операциялық жүйесі криминалист ғалымдар үшін маңызды сандық іздерді талдау және шығару үшін құнды құрал болып табылады.



# ЦИФРЛЫҚ ОРТАДАҒЫ СОТ САРАПТАМАСЫНЫҢ МАҢЫЗЫ

## Сандық дәлелдер

Цифрлық ғасырда криминалистика цифрлық дәлелдемелерді жинау мен талдауда маңызды рөл атқарады. Смартфондар, компьютерлер және планшеттер сияқты электрондық құрылғыларда қылмыстық әрекеттерге жарық түсіретін көптеген құнды деректер бар.



## Киберқылмыстарды зерттеу

Кибершабуылдардың және басқа да киберқылмыстардың таралуы сот-медициналық сараптаманы осы оқиғаларды тергеу үшін маңызды етеді.



## Алдын алу және тергеу

Криминалистика қылмыстарды тергеуде ғана емес, олардың алдын алуда да маңызды рөл атқарады. Сот-медициналық әдістер арқылы алынған деректерді талдау қылмыстық әрекеттегі үлгілер мен үрдістерді анықтауға көмектеседі.





# САНДЫҚ ІЗДЕРДІ ТАЛДАУДАҒЫ IOS 13 ОПЕРАЦИЯЛЫҚ ЖҮЙЕСІНІҢ РӨЛІ

## Mission



IOS 13 операциялық жүйесі сандық құрылғылардың криминалистикасында маңызды рөл атқарады. Бірегей архитектурасы және құпия деректерді күшті қорғауымен iOS 13 сандық криминалистика мамандары үшін айтарлықтай қиындық тудырады. Файлдық жүйені, iOS 13 метадеректерін және артефактілерін мұқият талдау қылмысты тергеу үшін маңызды болуы мүмкін маңызды дәлелдерді алуға мүмкіндік береді.

Шифрлау механизмдерін, пайдаланушы әрекетінің журналдарын, қызметтік дерекқорларды пайдалануды және iOS 13 жүйесіндегі қолданбалардың өзара әрекеттесуін тексеру сот сараптамасының негізгі аспектілері болып табылады. Бұл оқиғалардың суретін қайта құруға, заңсыз әрекеттердің іздерін анықтауға және сотта ұсынылуы мүмкін бұлтартпас дәлелдерді алуға мүмкіндік береді.

## Vision



# IOS 13 ҚҰРЫЛҒЫЛАРЫНАН ДЕРЕКТЕРДІ ШЫҒАРУҒА АРНАЛҒАН ҚҰРАЛДАР

Арнайы деректерді шығару құралдары iOS 13 құрылғыларының криминалистикалық талдауында маңызды рөл атқарады. Бұл қолданбалар мен бағдарламалық құралдар цифрлық дәлелдемелердің қауіпсіздігін қамтамасыз ете отырып, iPhone, iPad және iOS 13 жүйесімен жұмыс істейтін басқа құрылғылардан ақпаратты логикалық және физикалық түрде көшіруге мүмкіндік береді.

- Cellebrite UFED және Oxygen Forensic Detective сияқты кешенді сот сараптамасы шешімдері қуатты деректерді алуды, файлдық жүйені талдауды және жойылған ақпаратты қалпына келтіру мүмкіндіктерін қамтамасыз етеді.
- iTunes және iCloud Backup Extractor сияқты арнайы құралдар iOS құрылғысының сақтық көшірмелерінен деректерді логикалық түрде көшіруге мүмкіндік береді, бұл фотосуреттерге, контактілерге, хабарларға және басқа да құнды ақпаратқа қол жеткізуге мүмкіндік береді.
- XRY және MOBILedit Forensic сияқты жетілдірілген шешімдер құпия және шифрланған деректерді шығаруды қоса, төмен деңгейлі файлдық жүйеге кіру арқылы iOS құрылғыларынан физикалық деректерді шығаруға мүмкіндік береді.

Сот сарапшыларының осы құралдарды дұрыс пайдалануы тергеу кезінде iOS құрылғыларынан алынған сандық дәлелдемелерді сәтті жинау мен талдаудың кілті болып табылады.

# ФИЗИКАЛЫҚ ЖӘНЕ ЛОГИКАЛЫҚ МӘЛІМЕТТЕРДІ АЛУ ӘДІСТЕРІ

## ФИЗИКАЛЫҚ

Бұл барлық деректердің, соның ішінде құрылғыда жойылған немесе шифрланған деректердің толық көшірмесін алуға мүмкіндік береді. Ол үшін iOS құрылғысына қосылатын және бүкіл жадтың биттік көшірмесін жасайтын арнайы аппараттық құрылғылар пайдаланылады.

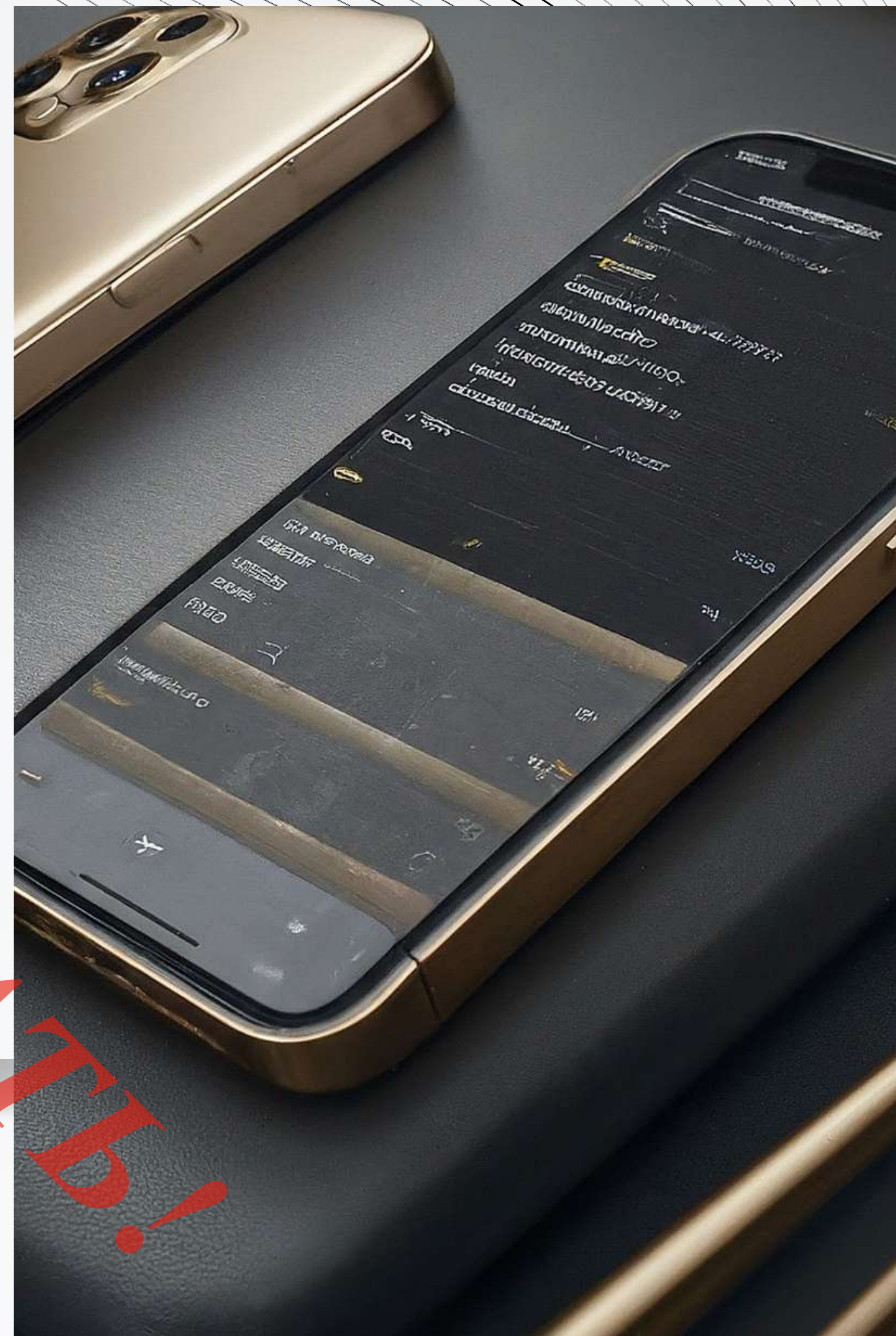
## ЛОГИКАЛЫҚ

Бұл файлдық жүйеге, дерекқорларға және құрылғының басқа құрылымдық деректеріне қол жеткізуге мүмкіндік береді. Бұл әдіс аз еңбекті қажет етеді және күрделі жабдықты қажет етпейді, бірақ сонымен бірге ол жойылған немесе шифрланған кейбір артефактілер мен деректерді жіберіп алуы мүмкін.



# IOS\_13 ФАЙЛДЫҚ ЖҮЙЕСІН ТАЛДАУ

Сандық криминалистика мамандары iOS 13 файлдық жүйесін талдау үшін әртүрлі әдістер мен құралдарды пайдаланады, бұл құпия құрылғы деректеріне қол жеткізе алатын және жойылған файлдарды қалпына келтіре алатын коммерциялық және ашық бастапқы бағдарламалық құралды пайдалануды қамтуы мүмкін. IOS файлдық жүйесінің құрылымын, сондай-ақ оның мүмкіндіктері мен нюанстарын терең түсіну сот сараптамасының осы түрін тиімді жүргізу үшін өте маңызды.





# МЕТАДЕРЕКТЕРДІ ТАЛДАУ



Метадеректер iOS 13 құрылғыларының криминалистикалық талдауында маңызды рөл атқарады, мысалы, жасалған күні, авторы, түсіру орны және басқа контекстік ақпарат сияқты файл метадеректерін егжей-тегжейлі тексеру сот сарапшыларына суретті қайта құруға мүмкіндік береді.

**МЕТАДЕРЕКТЕРДІ  
ЗЕРТТЕУ**



iOS 13 құрылғыларынан метадеректерді алу үшін сот сарапшылары операциялық жүйенің ішкі дерекқорларына қол жеткізуге мүмкіндік беретін арнайы бағдарламалық құралды пайдаланады.

**ШЫҒАРУ ЖӘНЕ ТАЛДАУ**

# СОТ ІСІН ЖҮРГІЗУДЕ КРИМИНАЛИСТИКАЛЫҚ ӘДІСТЕРДІ ҚОЛДАНУ

IOS 13 құрылғыларындағы  
цифрлық іздерді талдауға  
арналған  
криминалистикалық  
әдістер сотта рұқсат етілген  
және бұлтартпас  
дәлелдемелерді  
қамтамасыз етуде маңызды  
рөл атқарады.

**ДӘЛЕЛДЕМЕЛЕР  
БЕРУ**

Сандық дәлелдемелердің  
шығу тегі мен сенімділігі  
туралы пікірлерін беріп,  
судьялар мен алқабилерге  
негізделген қорытындыға  
келуге көмектеседі.

**СОТ САРАПТАМАСЫ**

IOS 13-тің  
криминалистикалық  
сараптамасы сонымен  
қатар құрылғыны  
пайдаланушының  
мінез-құлқын зерттеуге  
мүмкіндік береді.

**ПАЙДАЛАНУШЫНЫҢ  
МІНЕЗ-ҚҰЛҚЫН  
ЗЕРТТЕУ**

# САНДЫҚ ІЗДЕРДІ АЛУ ҮШІН ФАЙЛДАР МЕН ДЕРЕКҚОРЛАРДЫ ЗЕРТТЕУ

## IOS 13 ФАЙЛДЫҚ ЖҮЙЕСІ

IOS 13 құрылғыларының файлдық жүйесін мұқият талдау сот-медициналық тергеудегі негізгі қадам болып табылады. Сарапшылар файлдардың әртүрлі түрлерін, соның ішінде мәтіндік құжаттарды, фотосуреттерді, бейнелерді, дауыстық хабарларды және құрылғыда сақталған басқа деректерді зерттей алады. Бұл файлдардың жасау, өзгерту және соңғы кіру күндері сияқты метадеректерін талдау пайдаланушы әрекеті туралы маңызды ақпаратты бере алады және оқиғалар хронологиясын қайта құруы мүмкін.

## IOS 13 ДЕРЕКҚОРЛАРЫ

ios 13 операциялық жүйесі пайдаланушының контактілері, хабарлары, күнтізбесі, орналасқан жері және басқа да жеке мәліметтері туралы ақпаратты сақтау үшін көптеген ішкі дерекқорларды пайдаланады. Криминалист ғалымдар құнды дәлелдер алу үшін осы дерекқорларды шығару және талдау үшін арнайы құралдарды пайдалана алады. Мысалы, байланыс дерекқорында күдіктінің байланыстары туралы ақпарат болуы мүмкін, ал геолокация дерекқорында белгілі бір уақыт нүктелеріндегі орын туралы ақпарат болуы мүмкін.

## ЖАСЫРЫН ДЕРЕКТЕР

ios 13 құрылғыларындағы жасырын немесе жойылған деректерді зерттеу маңызды. Пайдаланушылар файлдарды немесе деректерді жою арқылы дәлелдерді жасыруға әрекет етуі мүмкін. Дегенмен, сот сарапшылары бұл ақпаратқа қол жеткізу үшін арнайы экстракция әдістерін пайдалана алады. Журналдарды, кэштерді, уақытша файлдарды және басқа деректер құрылымдарын талдау жасалған қылмысқа жарық түсіретін құнды цифрлық іздерді аша алады.