CyberLab
Комп'ютерна криміналістика

ЦИФРОВА КРИМІНАЛІСТИКА

Лабораторія комп’ютерної криміналістики

Цифрова криміналістика (Комп’ютерно–технічна експертиза)

Прикладна наука про відновлення та дослідження даних на цифрових пристроях, які можуть бути доказами у злочинах (інцидентах), пов'язаних із інформацією в електронному вигляді.

Комп’ютерна криміналістика

Вилучення та аналіз даних з усіх типів цифрових носіїв, включаючи видалені, приховані, шифровані й закриті паролями дані

Мобільна криміналістика

Вилучення інформації з мобільних пристроїв, навігаторів та іншої портативної техніки. Аналіз дій користувача, побудова взаємозв'язків

Мережева криміналістика

Дослідження несанкціонованого втручання в системи і мережі, в тому числі аналіз шкідливого та шпигунського програмного забезпечення. Фіксація та вилучення даних з онлайн сервісів чи Веб–ресурсів

Авто–комп’ютерна криміналістика

Дослідження блоків керування автомобів

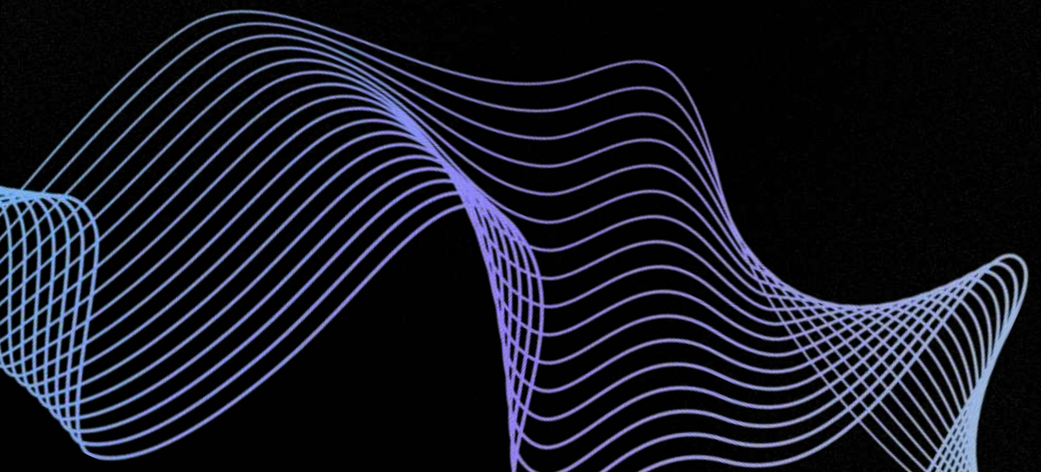
Комп’ютерно–технічна експертиза об’єкт–предмет

Об’єкти комп’ютерно–технічної експертизи:

– комп’ютерні носії інформації (накопичувачі на жорстких магнітних дисках, твердотільні накопичувачі, флеш–накопичувачі, диски для лазерних систем зчитування), сервери, системні блоки персональних комп’ютерів, портативні комп’ютери, планшетні комп’ютери, мобільні пристрої, відеореєстратори, GPS–навігатори, смарт–годинники, хмарні сховища, сторінки Інтернет ресурсів, файли користувача та службові файли програмного забезпечення, термінали самообслуговування та гральні автомати, тощо.

Предмет комп’ютерно–технічної експертизи складає певна група специфічних закономірностей, особливостей та ознак матеріальних об’єктів.

Тобто до предмету можна віднести інформацію та процеси, які відбувалися з нею.



Комп’ютерно–технічна експертиза завдання

До основних завдань комп’ютерно–технічної експертизи належать:

– установлення робочого стану комп’ютерної техніки;

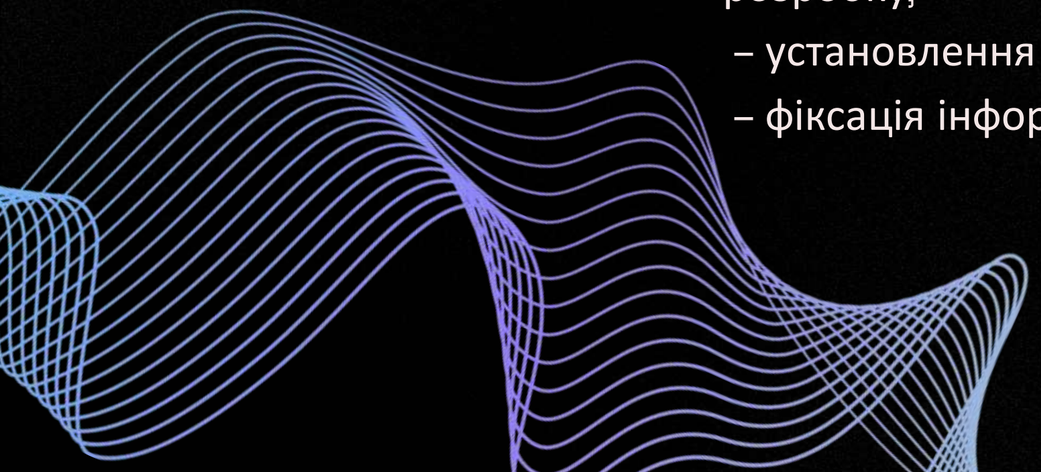
–установлення обставин, пов’язаних з використанням комп’ютерно–технічних засобів, інформації та програмного забезпечення;

– пощук виявлення інформації та програмного забезпечення, що містяться на комп’ютерних носіях;

– установлення відповідності програмних продуктів певним версіям чи вимогам на їх розробку;

– установлення функціональних можливостей програмних продуктів;

– фіксація інформації на Веб–ресурсах.



Комп’ютерно–технічна експертиза питання

Наказ **53/5** від **08.10.1998 «**Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково–методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень**»**

ПЕРЕЛІК ОРІЄНТОВНИЙ

Комп’ютерна криміналістика питання

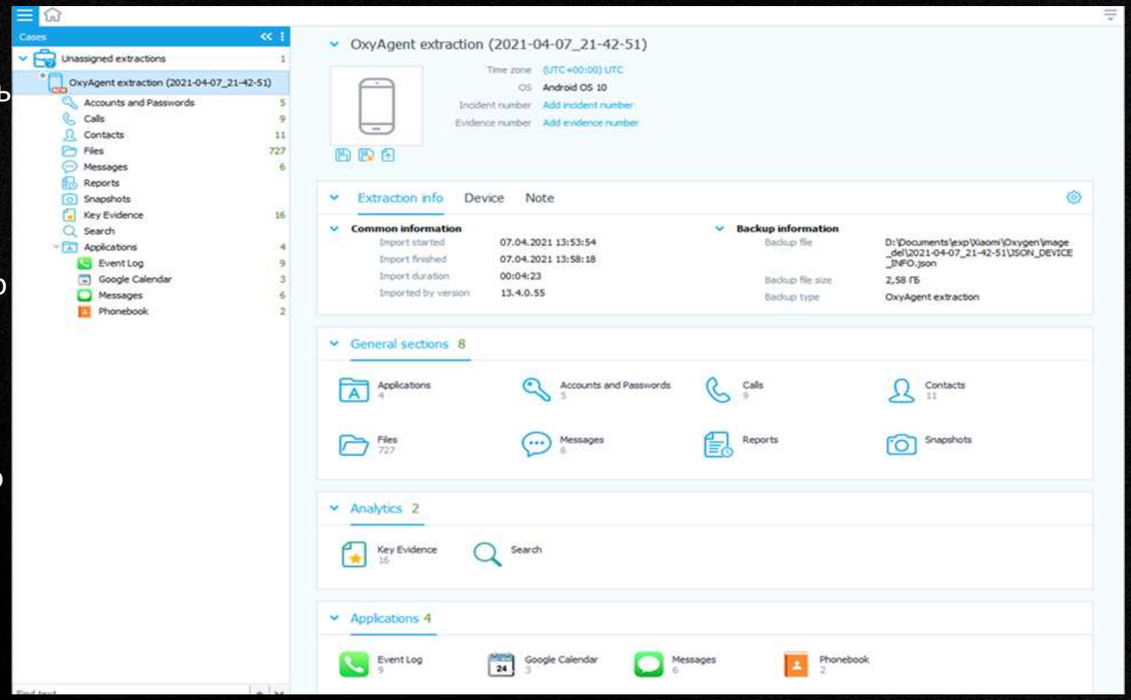
Перелік питань не є вичерпним

- Чи відбувалося підключення зовнішніх носіїв інформації до комп’ютера? Якщо так, то яких і коли саме?
- Чи є в пам’яті об’єктів файли, що містять в собі ключові слова «...», «...»? В разі наявності скопіювати зазначену інформацію на окремий носій.
- Чи містяться в пам’яті об’єктів файли формату «.doc», «.docx», «.pdf», «.xls», «.xlsx» та ін.? В разі наявності скопіювати зазначену інформацію на окремий носій.
- Яка технологія та хронологія створення електронного документа?
- Чи могла бути створена зазначена інформація на цьому комп’ютері чи вона перенесена з іншого носія?
- Чи міститься на наданому об’єкті графічні файли та відеофайли, у тому числі й видалені? В разі наявності скопіювати зазначену інформацію на окремий носій.
- Чи містяться на наданому відеореєстраторі відеозаписи, створені в період часу (вказати дату та час, за які потрібні відеозаписи)? Якщо так, то виявлені відеозаписи прошу скопіювати на окремий носій.
- Чи встановлені на наданих об’єктах програми, призначені для спілкування в мережі Інтернет («Viber», «Skype», «Telegram», «WhatsApp» та інші)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?
- Чи містяться на наданих об’єктах певне (зазначити назву або функціональне призначення, а також вид – встановлене чи не встановлене) програмне забезпечення? (у відношенні грального бізнесу – програми «iConnect», «iChampion», «G-slot», «Gaminator», «Superomatic», «iGaming Casino», «Megasuperomatic»)?
- Чи можливо виконання певних дій за допомогою даного програмного продукту?
- Чи можливе вирішення певного завдання за допомогою даного програмного продукту?
- Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?
- Чи міститься в пам’яті об’єктів програмне забезпечення, яке ідентифікується антивірусним програмним забезпеченням, як шкідливе? Якщо так, то до якого типу шкідливого програмного з забезпечення воно відноситься і яке його функціональне призначення?
- Чи міститься в пам’яті об’єктів файли з функціональними можливостями, характерними для шкідливих програмних засобів?

Мобільна криміналістика питання

Перелік питань не є вичерпним

- Чи містяться в пам’яті мобільного пристрою інформація щодо списку контактів, журналу дзвінків, текстових та мультимедійних повідомлень, веб–історії, повідомлень в мережі Інтернет, а також текстових, графічних, відео файлів користувача? При наявності зазначеної інформації прошу скопіювати на окремий носій інформації.
- Чи містяться в пам’яті мобільного пристрою, месенджери («Viber», «Skype», «Telegram», «WhatsApp» та інші)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?
- Чи міститься в пам’яті мобільного пристрою, програмне забезпечення, яке ідентифікується антивірусним програмним забезпеченням, як шкідливе? Якщо так, то до якого типу шкідливого програмного з забезпечення воно відноситься і яке його функціональне призначення?
- Чи міститься в пам’яті мобільного пристрою, додатки з функціональними можливостями, характерними для шкідливих програмних засобів?



Мережева криміналістика питання

Перелік питань не є вичерпним

- Чи містяться в пам’яті наданих об’єктів файли листів електронної пошти? В разі наявності скопіювати зазначену інформацію на окремий носій.
- Чи наявна в пам’яті наданих об’єктів історія відвідування Інтернет сторінок, пошукових запитів в мережі Інтернет, закладки веб–браузерів тощо?
- Чи містяться в пам’яті наданих об’єктів облікові дані (логіни та паролі) для доступу до Інтернет ресурсів?
- Чи міститься в пам’яті наданих об’єктів програмне забезпечення, елементи програмного коду або сліди використання програмного забезпечення, призначеного для віддаленого керування комп’ютером? Якщо так, то чи містить вказане програмне забезпечення лог–файли його використання?
- Чи наявні в пам’яті наданих об’єктів програми (клієнти) для дистанційного банківського обслуговування (ДБО) типу «Клієнт–банк» (вказати які саме),«Інтернет–банкінг» (вказати які саме)? Якщо так, то чи містять вони лог–файли використання вказаних програм?
- Чиміститьсяінформація, а саме (вказується конкретна інформація, а саме ключові слова, певні фото–відеозображеннячизображеннялоготипів) на Веб–ресурсі «.....»?

Авто–комп’ютерна криміналістика питання

Перелік питань не є вичерпним

- Чи містяться в пам’яті блока керування автомобіля інформація стосовно його пересування у відповідності до геолокації на мапі?
- Чи містяться в пам’яті блока керування автомобіля інформація щодо списку контактів, журналу дзвінків, текстових та мультимедійних повідомлень, веб–історії, повідомлень в мережі Інтернет, а також текстових, графічних, відео файлів користувача? При наявності зазначеної інформації прошу скопіювати на окремий носій інформації.
- Чи містяться в пам’яті блока керування автомобіля інформація стосовно месенджерів («Viber», «Skype», «Telegram», «WhatsApp» та інші)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?
- Чи містяться в пам’яті блока керування автомобіля інформація стосовно дій водія (гальмування, відкриття–закриття дверей, швидкість, тощо)?

Програмно–апаратні комплекси, як основний засіб:

X-Ways

Passware

MAGNET FORENSICS

MOBILedit Forensic Express

ACCESSDATA

OXYGEN FORENSICS

Типові помилки при формуванні питань до експертизи

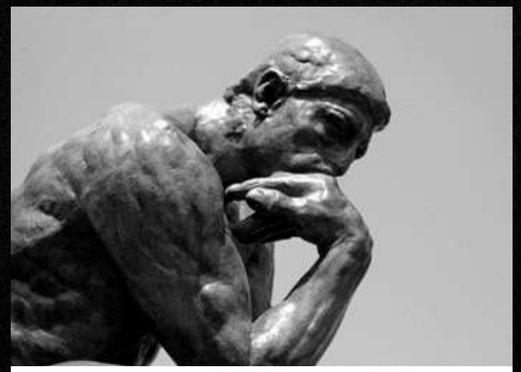
Питання, що покладають на експерта збір матеріалів / доказів

- Хто є користувачем мобільного телефону, номер мобільного телефону якого зазначений у месенджері
- Встановити, хто створив певну інформацію

Вирішення питань права (кваліфікація злочину)

- Чи був несанкціонований доступ до обладнання
- Чи відноситься обладнання до того, за допомогою якого можливо проводити азартні ігри

Типові помилки при формуванні питань до експертизи



Загальні питання

- Чи можливо змінювати дату
- Яка міститься інформація і яке її цільове призначення
- Чи є наявність / відсутність інформації передумовою для...

«Неправильні» матеріали та об'єкти досліджень

- Фото комп’ютерної техніки
- Скриншоти, окремі файли
- Модифіковані об'єкти дослідження (переустановлена система, тривала робота після інциденту)

Розслідування vs експертизи

Розслідування / реагування на інцидент

Збір доказів / матеріалів
Вибір об'єктів для дослідження
Версії та їх перевірка

Дослідження вибраних об'єктів
Робота в команді із «замовником»

Комп’ютерно–технічна / телекомунікаційна експертиза

Прямо заборонено

Збір доказів / матеріалів
Вибір об'єктів для дослідження
Обґрунтований та об’єктивний письмовий висновок на поставлені питання

Дослідження усіх об'єктів
Незалежність

Підготовка до комп'ютерно–технічої експертизи

Визначити перелік об'єктів

Вибрати комп'ютери, телефони, інші пристрої, на яких може міститися інформація, яка має значення для справи

Створити копії та/або провести огляд

Зафіксувати спосіб та отриману інформацію у протоколі/акті –
створити «документ» в понятті КПК.

Сформувати перелік питань

З метою визначення, які саме об'єкти слід надати експерту, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста).

Не потрібно:

Видаляти (особисті) файли, віруси і т.ін.
Перевстановлювати операційну систему
Фотографувати телефони, робити скриношти і т.ін.

CyberLab
Комп'ютерна криміналістика

Збір та аналіз цифрових даних потребують спеціальних знань

Спосіб отримання доступу до інформації визначає об'єм та зміст даних

Немає задач, що не вирішуються, є неправильно сформовані задачі

ПОШТА	info@cyberlab.ua
САЙТ	cyberlab.ua
тел.	+380 (93) 904-9202 +380 (44) 338-3231