Partnership for Good Governance
Партнерство заради належного врядування

EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

НАЦІОНАЛЬНА ШКОЛА СУДДІВ УКРАЇНИ
NATIONAL SCHOOL OF JUDGES OF UKRAINE

Партнерство заради належного врядування РЄ/ЄС (ПНВ)

«Боротьба з корупцією та зміцнення належного врядування/

Боротьба з відмиванням грошей»

(EaP-2)

ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС РОЗГЛЯДУ СПРАВ, ПОВ'ЯЗАНИХ З КОРУПЦІЄЮ

Збірка навчальних матеріалів тренінгу для суддів

Розробники:

Стівен Браун, Овсянніков В.С., консультанти Ради Європи, Шинкоренко С.В. член робочої групи Національної школи суддів України

ECCD-PGG-UA-TP-03/2018 Дата: жовтень 2019

Ця збірка навчальних матеріалів тренінгу розроблена робочою групою Національної школи суддів України та експертами в рамках проекту Партнерства заради належного врядування РЄ/ЕС «Боротьба з корупцією та зміцнення належного врядування/Боротьба з відмиванням грошей» за фінансування Європейського Союзу та Ради Європи.

УДК 343.14:342.841

Рекомендувала до друку Науково-методична рада Національної школи суддів України (протокол № 6 від 01 жовтня 2019 року).

За науковою редакцією **Шукліної Наталії Георгіївни**, проректора Національної школи суддів України, к.ю.н., професора, заслуженого юриста України та **Іщенка Олександра Петровича**, заступника начальника відділу науково-методичного забезпечення діяльності судів та органів суддівського врядування Національної школи суддів України, к.ю.н.

За подальшою інформацією звертайтесь:

Відділ протидії економічній злочинності та співпраці
Департамент протидії злочинності
Генеральний директорат з прав людини та верховенства права
Рада Європи
67075 Страсбург CEDEX, Франція
Тел.: +33 (0)3 90 21 28 44
Факс: + 33 3 88 41 27 05
Email: Zahra.AHMADOVA@coe.int

Національна школа суддів України
Самофал Марина Михайлівна, заступник начальника відділу науково-методичного забезпечення діяльності судів та органів суддівського врядування Національної школи суддів України
вул. Жилянська 120А, Київ, 01032, Україна
Тел.: (044) 597 09 26,
Email: metod.vrj@nsj.gov.ua.

ЗМІСТ

ЗМІСТ **3**

ПЕРЕЛІК СКОРОЧЕНЬ **6**

1 АНОТАЦІЯ **7**

2 ПРОГРАМА ТРЕНІНГУ **8**

3 ВСТУП **10**

4 ПРИРОДА ЕЛЕКТРОННИХ ДОКАЗІВ **11**

4.1 Що таке доказ? 11
4.2 Джерела електронних доказів 12
4.3 Сліди активності в онлайні 16
4.4 Важливі особливості електронних доказів 17
4.5 Типи пам'яті 17
4.6 Зовнішні портативні пристрої 18
4.7 Хмара 19
4.8 Нулі та одиниці 20
4.9 Мережі 22

5 МЕРЕЖА ІНТЕРНЕТ: ПРИНЦИПИ ФУНКЦІОНУВАННЯ **25**

5.1 Кількість користувачів 25
5.2 Складові мережі Інтернет 25
5.3 Маршрутизація 26
5.4 Категорії Даних: 26
5.5 URL (Єдина вказівка ресурсу) 27
5.6 IP адреси 29
5.7 Шістнадцяткова система числення 29
5.8 Статична та динамічна IP адреси 30
5.9 Whois 30
5.10 Машина Wayback 31
5.11 Відстеження IP адреси 31
5.12 Хмара 32
5.13 Програмне забезпечення для анонімізації 33

6 ТЕЛЕФОНИ ЯК ДОКАЗ **35**

6.1 Телефонна залежність 35
6.2 SIM 36
6.3 Обсяг пам'яті 36
6.4 З'єднання 37
6.5 GPS 39
6.6 Перехоплювачі IMSI 39

7 СУДОВА ЕКСПЕРТИЗА ЕЛЕКТРОННИХ ДОКАЗІВ **41**

7.1 Можливості цифрової криміналістики 41
7.2 Електронні докази у випадках корупції 41
7.3 На місці злочину 42

7.4 Активні пристрої....42
7.5 Неактивні пристрої....45
7.6 Пакети Фарадея....46
7.7 Шифрування....48
7.8 Зламування....49
7.9 Основні закони про розкриття інформації....51
7.10 ФБР проти Apple....51
7.11 Зламування правоохоронними органами....53

8 СПОСОБИ ВИЯВЛЕННЯ ПРИХОВАНИХ ФАЙЛІВ....55

8.1 Що відбувається у лабораторії?....55
8.2 Хешування....55
8.3 Зберігання даних....59
8.4 Різні файлові системи....63
8.5 Приховування файлів....64
8.6 Стеганографія....65
8.7 Журнали....67
8.8 Історія перегляду веб-сторінок....68
8.9 Журнали веб-серверів....72
8.10 Дані з Exchangeable Image Format (EXIF)....74
8.11 Електронні листи:....75
8.12 Інструменти цифрової криміналістики....77

9 ОСНОВНІ ЗАСАДИ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В УКРАЇНІ 79

9.1 Електронні докази: поняття, види....79
9.2 Особливості регулювання у КПК....81
9.3 Електронні документи....81
9.4 Веб-сайти (сторінки)....83
9.5 Проблеми фіксації інформації як доказу в мережі Інтернет....85
9.6 Приклади справ....90
9.7 Текстові, мультимедійні та голосові повідомлення....91
9.8 Запитання до аудиторії....92
9.9 Метадані....94
9.10 Бази даних....97

10 ДОПУСТИМІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ....99

10.1 Підстави допустимості....99
10.2 Питання якості....99

11 ТЕХНІЧНІ ТА ЮРИДИЧНІ ОСОБЛИВОСТІ КРИПТОВАЛЮТИ....102

11.1 Що таке криптовалюта?....102
11.2 Блокчейн....103
11.3 Зарубіжне регулювання криптовалют....103
11.4 Національне законодавство щодо регулювання криптовалют....104
11.5 Використання криптовалюти у відмиванні коштів або іншого майна, одержаних внаслідок вчинення суспільно небезпечного протиправного діяння....105

12 МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПРИ ЗБОРІ ЕЛЕКТРОННИХ ДОКАЗІВ....108

12.1 Національне регулювання міжнародної допомоги....108
12.2 Конвенція про правову допомогу та правові відносини у цивільних, сімейних і кримінальних справах 1993 року....110
12.3 Міжнародні угоди про надання правової допомоги....110
12.4 Регулювання міжнародної допомоги у КПК України....112
12.5 Докази постачальника послуг у США....113
12.6 Нова ініціатива ЄС....115

13 ЕЛЕКТРОННА ПОШТА....117

14 ВИСНОВКИ....126

15 ДОДАТКИ....127

15.1 Практичні вправи....127
Додаток 1. Практична вправа щодо використання даних геопозиції та координат базових станцій....127
Додаток 2. Практична вправа щодо перевірки дотримання процесуального закону при вилученні пристроїв та при подальших діях з електронними доказами....131
Додаток 3. Практична вправа із оцінки використання електронних доказів....132
Додаток 4. Практична вправа з оцінки допустимості доказів....134
Додаток 5. Практична вправа з питань міжнародного співробітництва щодо отримання та використання електронних доказів....135
15.2 Перелік презентацій....138

ПЕРЕЛІК СКОРОЧЕНЬ

КК України	Кримінальний кодекс України
КПК України	Кримінальний процесуальний кодекс України
ASCII	American Standard Code of Information Interchange, код для представлення символів алфавіту у вигляді чисел
CGNAT	Carrier Grade Network Address Translation, спосіб підключення до Інтернет мережі, де декілька пристроїв використовують одну IP адресу
HDD	Hard Disk Drive, жорсткий диск або вінчестер
HTTP(S)	Hypertext Transfer Protocol (Secure), протокол передачі гіпертексту
ICANN	Internet Corporation for Assigned Names and Numbers, організація, яка видає доменні імена
IMEI	International Mobile Equipment Identifier, індивідуальний номер мобільного обладнання
ISP	Internet Service Provider, Інтернет провайдер
MAC	Media Access Control, це унікальний ідентифікатор, який визначає пристрій всередині мережі
PUK	Personal Unlocking Key, код, за допомогою якого відновлюється доступ до заблокованого телефону
RAM	Random Access Memory, ОЗП – Оперативний Запам'ятовуючий Пристрій – вид комп'ютерною пам'яті, що швидко працює, але доступ до якої втрачається із вимкнення ПК
SDC	Secure Digital Card, СД картка
SSD	Solid State Drive, твердий жорсткий диск
TCP/IP	Transfer Control Protocol/Internet Protocol, стандартний протокол Інтернет мережі, що регулює трафік
URL	Uniform Resource Locator, назва сайту у літерному вираженні
USB	Universal Serial Bus, стандартний порт для підключення периферійних пристроїв
VPN	Virtual Private Network, Віртуальна Приватна Мережа

1 Анотація

В цьому виданні вміщені навчальні матеріали для суддів, які спеціалізуються на розгляді справ, пов'язаних з корупцією, про застосування електронних доказів та їх оцінку, а також про законодавче регулювання електронних доказів та міжнародне співробітництво в цій сфері.

Метою видання є розкриття поняття електронних доказів, особливостей їх застосування під час розгляду справ, пов'язаних з корупцією; роз'яснення національного законодавства в частині оцінки електронних доказів; забезпечення базового розуміння технічних аспектів роботи з електронними доказами та методами експертних досліджень; підвищення обізнаності щодо існуючих міжнародних договорів, які регулюють питання міжнародної правової допомоги, в тому числі щодо збору та передачі електронних доказів; демонстрація способів приховати електронні докази та методів боротьби з приховуванням; тренування суддів щодо вирішення спірних практичних питань застосування та оцінки електронних доказів. Ця публікація також спрямована на створення зв'язку з національним та міжнародним законодавством, оскільки вказаний вид злочину має транснаціональний характер.

Над розробкою працювала команда вітчизняних та зарубіжних фахівців, що дозволило розглянути в різних аспектах практичні та теоретичні проблемні питання застосування електронних доказів під час розгляду справ, пов'язаних з корупцією.

Автори сподіваються, що це видання сприйматиметься читачами як корисний інструмент, заохочуватиме до поглиблення знань та розуміння особливостей електронних доказів, що зумовлює необхідність перевірки допустимості таких доказів та розуміння особливостей їх застосування.

2 ПРОГРАМА ТРЕНІНГУ

День 1	
9.00-09.30	**Реєстрація учасників**
09.30-09.45	**Вітальне слово**
09.45-10.00	**Знайомство учасників** Ця сесія передбачає вступні пояснення щодо сутності тренінгу, методології його проведення, навчальних цілей, а також знайомство учасників і викладацької групи, пленарне обговорення учасниками своїх очікувань, досвіду застосування електронних доказів.
10.00-10.45	**Міні-лекція: "Природа електронних доказів"** Протягом міні-лекції буде здійснено аналіз специфічних ознак електронних доказів, їх відмінностей від традиційних доказів, джерел отримання електронних доказів, особливостей збору електронних доказів.
10.45-11.00	**Хвилинка здоров'я, кава-пауза**
11.00-11.45	**Міні-лекція "Мережа Інтернет: принципи функціонування"** Протягом міні-лекції буде презентовано загальні принципи функціонування мережі Інтернет з акцентом на доцільність та можливість використання відповідної інформації у судовому провадженні.
11.45-12.05	**Підготовка до практичної вправи (роз'яснення ключових елементів)**
12.05-13.00	**Практична вправа** щодо використання даних геопозиції та координат базових станцій для визначення місцезнаходження особи в певний час та використання цих даних в якості доказів у кримінальному провадженні.
13.00-14.00	**Перерва на обід**
14.00-15.00	**Міні-лекція "Судова експертиза електронних доказів "** У ході міні-лекції відбудеться висвітлення особливостей збору електронних доказів та їх достовірності.
15.00-15.15	**Хвилинка здоров'я, кава-пауза**
15.15-16.00	**Міні-лекція "Способи виявлення прихованих файлів"** Протягом міні-лекції будуть висвітлені основні аспекти, на які варто звернути увагу під час аналізу електронних доказів, та окреслена техніка, за допомогою якої зазвичай відбувається приховання електронних доказів.
16.00-16.40	**Практична вправа** щодо перевірки дотримання процесуального закону при вилученні пристроїв та при подальших діях з електронними доказами. Слідчим проведено обшук приміщення, внаслідок якого вилучено системний блок та смартфон. Необхідно перевірити дотримання процесуального закону при вилученні пристроїв та при подальших діях з електронними доказами.

День 2	
9.30 – 9.45	**Огляд першого дня**
09.45 –10.45	**Міні-лекція "Основні засади законодавчого регулювання електронних доказів в Україні".** Протягом міні-лекції буде висвітлено матеріальне і процесуальне законодавство у вказаній сфері.
10.45-11.30	**Практична вправа із оцінки використання електронних доказів**
11.30 – 11.45	**Хвилинка здоров'я, кава-пауза**
11.45 – 12.45	**Практична вправа з оцінки допустимості доказів** Вправа складається з декількох схожих за суттю завдань. Є підстави вважати, що під час допиту підозрюваного до нього застосовувалося фізичне насильство з метою дізнатись його пароль до зашифрованих на його ПК даних. Також наявні певні порушення при експертній роботі з електронними доказами. Слід встановити наявність або відсутність порушень та визначити, чи є отримані докази допустимими. Необхідно дати оцінку допустимості доказів, при роботі з якими експерт використав застаріле та неліцензійне програмне забезпечення. За наявності даних, що повідомлення, яке становить предмет доказування, відправлене з одного із декількох ПК, слід дати оцінку непрямим доказам щодо того, чи відправлено воно з конкретного ПК.
12.45 – 13.00	**Питання та відповіді**
13.00-14.00	**Перерва на обід**
14.00-14.20	**Міні-лекція "Технічні та юридичні особливості криптовалюти"** Протягом лекції буде висвітлено, що таке криптовалюта, особливості її законодавчого регулювання в Україні та інших країнах, а також її використання у відмиванні коштів.
14.20 -15.00	**Міні-лекція "Міжнародне співробітництво під час збирання електронних доказів"** Протягом міні-лекції будуть висвітлені особливості законодавства в частині регулювання міжнародної правової допомоги.
15.00 – 16.00	**Практична вправа з питань міжнародного співробітництва щодо отримання та використання електронних доказів**
16.00 – 16.30	**Підведення підсумків тренінгу** Обговорення змісту тренінгу, з'ясування вражень від застосування методики навчання, отримання побажань суддів.

3 Вступ

Для багатьох з Вас ця тема буде повністю новою і Ви, можливо, вважаєте комп'ютерні технології занадто складними. Не панікуйте! Це не технічний курс і він не вимагає, щоб Ви були математиком або комп'ютерним ученим. Навпаки, курс забезпечить Вас базовими знаннями та навиками щодо електронних доказів і як вони застосовуються у Вашій професійній діяльності. Курс надасть Вам знань як працювати з такими доказами в суді і як оцінювати їх упевнено та правильно.

Ви є фахівцями у кримінальному праві, тому розумієте важливість дотримання процедури та вимог допустимості доказів. Природа і характеристики електронних доказів вимагають від Вас певних навичок, але такі навички надають Вам очевидні переваги; не лише під час доказуванні вини, але і у виправданні невинного. Інформаційні технології становлять безпрецедентний виклик для усіх учасників юридичної системи. Закон є консервативним; він надає перевагу достатньому емпіричному досвіду. На жаль, високий темп інновацій та зміни інформаційних технологій запроваджують нестабільність у добре перевірені та усталені принципи та процедури системи правосуддя. Такі нововведення приголомшують і значно ускладнюють процес правозастосування. Інформаційні технології змінили наше життя, а також спосіб вчинення злочинів. Кримінальній юстиції потрібно не відставати!

4 ПРИРОДА ЕЛЕКТРОННИХ ДОКАЗІВ

Мета навчання:

Слухачі вивчатимуть визначальні характеристики електронних доказів та їх вплив на збір доказів.

Зміст:

- Відмінності між традиційними і електронними доказами
- Де можна знайти електронні докази
- Як все, що зроблено на комп'ютері, залишає сліди
- Вилучення даних та спір щодо конфіденційності
- Комп'ютери - тільки калькулятори
- Види комп'ютерної пам’яті:
  - оперативна та довгострокова
  - види зберігання даних
  - потенційні ушкодження, викликані непрофесійними діями
- Розширені межі місця скоєння злочину
- Мережі, сервери і маршрутизатори

4.1 Що таке доказ?

Давайте розпочнемо з визначення поняття «доказ».

Докази – це фактичні дані, отримані у передбаченому законом порядку, які свідчать про наявність чи відсутність фактів та обставин, що мають значення для провадження і підлягають доказуванню.

Докази стосуються усіх елементів складу правопорушення і повинні доводити поза розумним сумнівом, що обвинувачений скоїв правопорушення. Інколи достатньо трьох факторів - засобів, мотиву і можливості, але це тільки відправна точка. Доказ це що-небудь, що доводить або спростовує спірний факт. Воно повинно бути належним у справі; повинно бути повним і достовірним. Доказ має бути визнаним належним та допустимим, або бути виключеним; зазвичай доказ перевіряється відповідно до певних об'єктивних стандартів доказування. Доказування здійснюється різними методами, у тому числі:

1) допит свідків
2) висновки експертиз, допит експертів
3) допит обвинуваченого
4) зізнання

5) традиційні експертні засоби (наприклад відбитки пальця, ДНК-експертизи та інші)

6) письмові докази

7) речові докази

Доказ може бути прямим або непрямим. Він повинен бути належним, відповідати правилам допустимості. Доказ може бути фізичним об'єктом, наприклад пістолетом чи ножем, або бути документом. У будь-якому разі Ви, як суддя, хочете дослідити найкращий з можливих доказів - зазвичай оригінал чого-небудь - та бути здатним покластися на нього у вироку.

У корупційних справах часто бракує прямих доказів, оскільки учасники мають причини приховувати свої дії. Потерпілими є абстрактні держава та суспільство, а не конкретна фізична особа. Інколи такі справи викриваються, тому що одна із сторін противоправних відносин вважає, що інша сторона її обдурює, і звертається із заявою до правоохоронних органів, а іноді корупція просто є очевидною і привертає увагу під час певних перевірок. Докази вини в такому випадку часто будуть непрямі, наприклад підозрюваний має статки або інші активи, які він не зміг би придбати в межах офіційного доходу. Також є можливим, що підозрюваний зустрічався з певними змовниками і обговорював їх злочин або, можливо, є викривальний документ, який підозрюваний зберігає в якості страхування.

Електронні докази важко віднести до певної категорії доказів. Електронний доказ, в теорії, є непрямим, оскільки електронний пристрій – це тільки пристрій, що утримує доказові дані. У разі встановлення наявності доказових даних на пристрої, такі дані не тільки необхідно вилучити з нього, а і вжити заходів на підтвердження того, що саме ця конкретна особа використовувала вказаний пристрій у відповідний період часу.

Як і з традиційними формами доказів, злочинці спробують приховати свої дії. Технічно обізнаний злочинець може значно ускладнити розслідування.

4.2 Джерела електронних доказів

Будь-який електронний пристрій, який ви можете уявити, може зберігати дані, якщо він здатний зберігати записи своєї дії, і до такого запису є доступ. Такі пристрої не завжди очевидні. Широкий вибір пристроїв, що є доступними зараз, і їх можливість з'єднання з інтернетом значно підвищили можливості для з'ясування відомостей про певну особу. Проте, без дотримання правил та процедур роботи з такими даними, є також ризик, що доступ до такої інформації може порушити права людини.

Електронні докази звичайно можна знайти на всіх видах комп'ютерних пристроїв і їх зовнішніх пристроях, а також пристроях для зберігання інформації (як наприклад жорсткі диски, USB карти, CD-ROMи). Менш очевидні пристрої, які також можуть зберігати дані, це, наприклад, музичні плеєри та ігрові консолі.

Очевидні місця, де цифрові докази можуть бути знайдені:

1) комп'ютер, ноутбук або планшетні комп'ютери

2) портативні пристрої для зберігання інформації, наприклад CD диски, DVD диски, USB карти, зовнішні жорсткі диски

3) смартфони

4) цифрові фотоапарати

5) принтери

6) віддалене хмарне зберігання

7) маршрутизатори

У діловому середовищі електронні докази також зберігаються на сервері замість особистих пристроїв. Сервер - спеціальний комп'ютер, який забезпечує або 'обслуговує' інші комп'ютери у мережі 'послугами'. Вилучення даних із серверів у великій компанії може становити загрозу функціонування компанії, і необхідно дотримуватись балансу між збереженням доказів та невтручанням у роботу господарюючого суб'єкта. Такі сервери також можуть містити дані, що стосуються третіх сторін, які не є предметом розслідування, і мають права на конфіденційність та невтручання. Тобто, просто завантажити усі дані без виключення може бути неправильним.

Докази будь-якої підозрілої діяльності в інтернеті можуть також знаходитись на серверах, що належать постачальнику інтернет послуг або телекомунікаційній компанії (у випадку смартфону). У такому випадку доказ може бути у формі роздруківки логів або протоколу діяльності.

Враховуючи, що наразі наявна велика кількість взаємопідключених пристроїв, можна знаходити докази і в менш очевидних місцях:

1) Смарт колонки

Смарт колонки, такі як Амазон Ехо, стають дуже популярними. Вони активуються голосовими командами, і це означає, що вони «слухають». У 2016 році у США поліція шукала докази на таких колонках на місці вбивства, сподіваючись знайти звукозапис щодо вбивства.[1] У 2018 році той же вид пристрою записав приватну бесіду, але неправильно оцінив команди, і відправив запис бесіди особі зі списку контактів.[2]

2) Ігрові консолі (приставки)

Ігрові консолі – це фактично комп'ютерні телекомунікаційні пристрої, якщо вони підключені до Інтернету. Деякі ігри дозволяють людям зустрічатись у віртуальному світі, де вони мають уявну особу, яка називається Аватар. Спілкування відбувається у реальному часі і може проводитися де завгодно у світі. Такі онлайн-місця для зустрічі можуть використовувати як злочинці, так і терористи. Деякі держави вживають заходи для додаткового контролю таких способів спілкування. Наприклад, рада безпеки РФ доручила

[1] https://habr.com/post/400395/
[2] https://www.wht.by/news/comment/63397/

ФСБ ввести ідентифікацію користувачів онлайн ігор та соціальних мереж за допомогою мобільних телефонів у 2018 році.[3]

3) Іграшки

Wifi іграшки також можуть використовуватись в якості доказу, як і смарт колонки. У Німеччині лялька на ім'я «Мій друг Кейла» була заборонена, тому що може використовуватись в якості пристрою для шпіонажу.

Впливові групи у США подали об'єднану скаргу на такі іграшки до Федеральної Торгової Комісії, заявивши, що такі іграшки записують та зберігають приватні розмови малолітніх дітей без обмежень щодо зберігання, використання або розкриття персональних даних.[4]

4) Бодікамери

Ряд поліцейських служб у всьому світі видають бодікамери своїм поліцейським. Ці камери записують роботу інспекторів з громадянами, і можуть надати докази проступку або, навпаки, показати, що інспектор поводився правильно. Очевидно, що якщо запис відсутній, то це може свідчити про наявність вини інспектора.

5) Фітнес трекери

Фітнес трекери можуть допомогти встановити місцезнаходження особи у певний час, при цьому ці трекери мають значні недоліки в частині інформаційної безпеки. Американським військовим нещодавно було заборонено використовувати такі трекери.[5]

6) Смарт годинники

Смарт годинники – це фактично мінікомп'ютери. Вони можуть виконувати багато функцій. Вони не лише показують час, але і можуть бути використані як електронні ключі, можуть відправляти електронну пошту, управляти безпроводними пристроями і таке інше.

Випадок із вбивством журналіста Хашоггі яскраво ілюструє можливості смарт годинників щодо запису подій. Хашоггі мав на собі смарт годинник apple watch, синхронізований з його телефоном. Перед тим, як зайти в будівлю консульства Саудівської Аравії у Стамбулі, він передав свій телефон нареченій. Крім того, у нього була активована функція хмарного зберігання даних, і смарт годинник передав записи його вбивства на хмару.[6]

7) Смарт ТВ

Едвард Сноуден виявив, що існує комп'ютерна програма ЦРУ на ім'я 'Плачущий Ангел', яка може спостерігати, що ви робите через Samsung Смарт ТВ. Інші розвідувальні служби теж можуть мати такі програми.[7]

---

[3] https://habr.com/post/358052/
[4] https://www.cnet.com/news/kids-talking-toys-iot-internet-of-things-privacy-ftc/
[5] https://www.segodnya.ua/world/usa/amerikanskim-voennym-zapretili-polzovatsya-prilozheniyami-s-gps-1160550.html
[6] https://24tv.ua/ru/saudovskij_zhurnalist_zapisal_svoe_ubijstvo_na_apple_watch__tureckie_smi_n1047075
[7] https://hightech.fm/2017/03/09/cia-mi5-hacked-smart-tv

Взагалі, будь-який пристрій, в якому є функція голосового управління, постійно слухає всі звуки навколо і аналізує їх, шукаючи голосові команди. Залежно від конкретного пристрою записаний звук деякий час зберігається в пам'яті цього пристрою. Так само працює і функція впізнання обличчя в сучасних телефонах, які розблоковуються, коли власник на них дивиться. Очевидно, що для того, щоб розуміти, що на нього дивляться, він повинен візуально спостерігати за тим, що відбувається навколо за допомогою відеокамери.

8) Транспортні засоби

Минули часи, коли автомобіль був чисто механічною формою транспорту. Зараз вони виконують безліч електронних функцій. Деякі автомобілі містять мікропроцесори, які автоматично викликають постачальника послуг, коли виявляють несправність, інші мають вбудовані комп'ютери, системи GPS, камери приладової панелі, відеореєстратори. Зазвичай мікропроцесори в автомобілі можуть показати, коли і де засіб рухався.

У Китаї виробники електрокарів з 2016 року надають уряду інформацію про своїх клієнтів без їх відома. Більш ніж 200 автовиробників, включаючи Tesla, Volkswagen, BMW, Daimler, Ford, General Motors, Nissan, Mitsubishi та NIO передають уряду персональні дані покупців за, як мінімум, 61 параметром. Відстежується усе – маршрути, адреси, час зарядки та номер банківскої картки, номер телефона, електронна адреса тощо.[8]

9) Електронні рідери

Електронні рідери - планшетні комп'ютери для читання книг. Деякі можуть підключатись до інтернету, всі можуть зберігати файли.

10) Приховані флешкарти пам'яті

Карти можуть бути замасковані у інші побутові чи інші пристрої.

11) Електронні карти доступу

Електронні карти доступу часто використовуються на підприємствах для надання особі доступу до будівель, чи приміщень. Вони можуть бути використані, щоб показати, коли певна особа прийшла або пішла з роботи, а також для ідентифікації особи. Будь-яке використання таких карт реєструється, і інформація може бути з них вилучена. Такі карти також часто використовуються готелями як електронні ключі до номерів.

12) Побутові пристрої

Побутові пристрої, наприклад, мийні машини, все більше і більше з'єднуються з домашніми комп'ютерними мережами. Всі такі пристрої зберігають записи, коли вони використовувались. У одному розслідуванні вбивства факт, що пральна машина підозрюваного була незвично використана посеред ночі (і незабаром після часу смерті) був використаний на підтвердження вини, оскільки одяг підозрюваного був випраний.

13) Банкомати

[8] https://auto.24tv.ua/ru/v_kitae_mashiny_sledyat_za_grazhdanami_n9123

У банкоматах зберігаються відомості щодо їх кожного використання (логи). Крім того, все частіше дії з банкоматом фіксуються відеокамерою.

4.3 Сліди активності в онлайні

Уся активність в онлайні залишає певні сліди, які можна використати, щоб ідентифікувати підозрюваного. Це також відноситься до соціальних мереж.

Наприклад, для підтвердження факту, що пристрій в певний час використовувався конкретною особою, може бути корисною перевірка активності його сторінки в соціальній мережі. Небагато людей можуть утриматись від перевірки своєї сторінки в соцмережі. Перевірка входів на таких акаунтах може також допомогти встановити погляди особи або виявити можливих співучасників.

Є також програми, які дозволяють визначити певну зону на мапі, та виявляти усю соціальну медіа-діяльність в цій області. Це дає можливість знаходити докази або свідків події, яка є предметом дослідження у справі.

Наприклад, програма (www.echosec.net) Echosec може допомогти відстежити підозрюваних, знаходити свідків та несподівані відеодокази.

Демонстрація доступна на Youtube:

https://www.youtube.com/watch?v=1Loc128ppuE&app=desktop

У короткій відеодемонстрації ви можете побачити, як обирається область в міській місцевості і навколо визначеної зони інтересу здійснюється пошук соціальної медіа активності, такої як пости у фейсбуці чи твіттері.

Спочатку ви бачите різні пости у соціальній мережі та геолокацію цих постів. Потім можна обрати певний пост, і відкриється сторінка відповідної особи в соціальній мережі.

Цей інструмент демонструє, як популярність соціальних ЗМІ, викладання селфі фотографій та постів (повідомлень) про своє щоденно життя може також допомогти ідентифікувати потенційних свідків.

Сер Джефрі Восс, голова Верховного Суду Англії і Уельсу, - один з найвпливовіших суддів Англії і Уельсу, заявляв:

«Ми можемо фотографувати і ми фотографуємо, знімаємо відео і записуємо все, що відбувається з нами. Я думаю, у майбутньому буде значно менше спірних кримінальних справ, головним чином завдяки засобам спостереження. Більшість людей постійно носять свої смартфони із увімкненими геоданими. Вони роблять це добровільно, але якщо в майбутньому закон буде вимагати, щоб громадяни мали телефони при собі завжди, то уникати виявлення буде ще важче».

На думку судді Восс, сучасна тенденція фотографувати і пересилати кожен аспект щоденного життя створила нове джерело доказу, яке має безпосередній вплив на

встановлення фактів у справі, але звичайно, такі докази доведеться знайти, вилучити та оцінити, що є надзвичайно трудомістким завданням.[9]

4.4 Важливі особливості електронних доказів

При роботі з електронним доказом слід розуміти, що він є дуже непостійним; його легко змінити або знищити. Кожного разу, коли кнопка натискається або виконується дія на комп'ютерному або цифровому пристрої, змінюється його пам’ять. Деякі з цих дій автоматичні, деякі є нещасним випадком (наприклад внаслідок сильного магнітного поля), а інші є запланованими.

Той факт, що електронний доказ так легко змінити прямо впливає на оцінку його цілісності і означає, що спеціальні процедури мають бути дотримані при кожному їх зборі, зберіганні та обробці. Це також означає, що голлівудські фільми, які показують, як детектив шукає дані на комп'ютері чи смартфоні підозрюваного, є абсолютно невірними.

Як зазначалось раніше, електронний доказ по суті є непрямим, і розслідування повинне показати, що підозрюваний був фактичним користувачем пристрою в певний час.

Кожна дія на цифровому пристрої залишає певні сліди, а більшість програм автоматично формують звіти та мають реєстр виконаних дій (логи). Це використовується для доведення зв’язку між пристроєм та особою.

Проте, є реальний ризик, що доказові дані, що утримаються постачальником послуг, будуть видалені під час здійснення господарюючої діяльності. Перш за все, зберігання даних коштує постачальнику послуг грошей, і якщо компанії ці дані більше не потрібні (наприклад дані для виставляння рахунку клієнту і рахунок вже сплачено), компанія ймовірно їх видалить.

Це явище підштовхнуло ЄС до спроби прийняти законодавче регулювання та зобов’язати всіх постачальників цифрових послуг в країнах – членах ЄС зберігати всі дані за період від 6 до 18 місяців. Проте, Європейський Суд Справедливості з цього питання постановив, що Директива ЄС занадто широка і нерозбірлива; порушує право на приватне життя, вимагаючи зберігання даних щодо дій, які не заборонені кримінальним законом.

4.5 Типи пам’яті

ОЗУ або оперативна пам’ять схожа на короткочасну пам’ять людини. Вона використовує програмне забезпечення і обробляє дані та інформацію під час безпосередньої роботи. Розмір пам'яті визначає обсяг інформації і кількість завдань, які комп’ютер може виконати за один раз. Ця інформація є нестабільною; вона зникає як тільки вимикається енергопостачання комп’ютера.

Довгострокова пам'ять функціонує подібно до думки, ідеї чи досвіду, які ви добре пам’ятаєте і можете пригадати, коли думаєте про них. Зазвичай цю функцію виконує жорсткий диск (вінчестер), він має велику ємність і зберігає дані після вимкнення пристрою до безпосереднього видалення даних користувачем.

[9] https://www.lawgazette.co.uk/law/tech-will-see-the-end-of-contested-trials-says-vos-/5066050.article

Слід відмітити, що останнім часом стає популярною практика зменшення ємності жорстких дисків, виходячи з того, що користувач буде зберігати більшість даних на хмарі. Така практика дійсно є зручною за наявності надійного інтернет зв'язку. Хмарне зберігання означає, що дані зберігаються на спеціальному сервері, зазвичай в іншій країні, а Ви маєте до них доступ. Це зручно також і тому, що доступ до цих даних Ви маєте з усіх своїх пристроїв.

4.6 Зовнішні портативні пристрої

Флешкарти

Флеш карта пам'яті (флешка) – це зовнішній пристрій для зберігання даних, який підключається через порт USB. Вона не має ніяких рухомих частин і зберігає дані після виключення постійно. На теперішній час такі карти мають значну пам'ять, обсягом до 2 Терабайтів (2048 гигабайт). Як вже зазначалось раніше, вони можуть бути замасковані під інші речі або пристрої.

Безпечні цифрові карти

Безпечна цифрова карта (СД карта) - також зовнішній пристрій для зберігання даних. Вони, зазвичай, використовуються у цифрових відео або фото камерах, але деякі комп'ютери мають спеціальні порти для підключення таких карт. Існують також мікро СД карти, розміром з ніготь, але вони здатні утримувати значний обсяг даних (карти обсягом 200 Гб доступні у продажу). Такі карти дуже легко приховати.

Дискети

Зараз дискети є архаїчним засобом зберігання інформації, але вони загально використовувались тільки 20 років тому. Вони могли тримати близько 2 МБ інформації.

Оптичні диски

Оптичні диски виготовляють із полікарбонату, а дзеркальну поверхню із алюмінію та/або золота. Оптичні диски це або компакт диски (CD диски), або ДВД (DCD) диски. Обидва диски можуть бути або придатні тільки для читання, або для одноразового запису (такі диски мають помітку R), або для багаторазового запису (RW). Також вони можуть бути односторонніми та двосторонніми. Максимальний обсяг компакт диску 700 Мб, а DVD може утримати 4.7 Гб (а деякі спеціальні види дисків ще більше). Ми обговоримо метод зберігання даних на дисках згодом. На сьогодні оптичні диски вже вважаються застарілою технологією.

Зовнішні жорсткі диски

Зовнішні жорсткі диски стають все більш популярними і використовуються для резервного зберігання даних на комп'ютері або як основний засіб зберігання даних на пристрою із обмеженою ємністю запам'ятовуючого пристрою. Ці зовнішні жорсткі диски з'єднуються з пристроєм кабелем, зазвичай кабелем USB, і можуть мати ємність декількох Тб.

Тут буде доцільним пригадати закон Мура, який був одним із засновників головного виробника мікрочипів, компанії Інтел. Він висловив припущення, що кількість транзисторів на кристалі мікросхеми буде подвоюватися кожні 24 місяці. Створивши графік зростання продуктивності запам'ятовуючих мікросхем, він виявив закономірність: нові моделі мікросхем розроблялися через більш-менш однакові періоди (18-24 міс.) після появи їхніх попередників. При цьому їхня місткість зростала щоразу приблизно вдвічі. Це було в 1965 і доки ще його пророцтво збувається.[10]

Наведена нижче таблиця показує, скільки даних зберігається на носії залежно від типу таких даних.[11]

Тип даних або документу	Середня кількість сторінок	
	1 Мб	1 Гб
Текст	662	677,963
Емейл	97	100,099
Зображення	15	15,477
Microsoft Word	63	64,782
Microsoft PowerPoint	17	15,552
Microsoft Excel	161	165,791

Таким чином, на 32 Гб СД картці або флешкарті можна зберігати 2 073 024 сторінки у Microsoft Word, або 495 264 зображення. Але слід пам'ятати, що не тільки можливості зберігання даних зростають кожні 18 місяців, а і програмне забезпечення стає більш складним та потребує більше ресурсів для роботи. Наприклад, якщо порівняти можливість зберігання просто тексту із його зберіганням в форматі Microsoft Word, можна побачити, що простий текст займає в 10 разів менше місця.

4.7 Хмара

У хмарних обчисленнях дані тримаються в серверних фермах. Великі корпорації утримують такі хмари - склади, повні серверів. Ймовірно, що хмарні дані клієнта перебувають в іншій країні, а сервер може бути де завгодно, від арктичного кола до підводного розташування (де зовнішнє середовище допомагає охолоджувати неймовірну спеку, яку створює велика кількість електроніки).

При використанні хмари у деяких випадках пристрій користувача функціонує майже виключно як екран і клавіатура, а опрацьовані дані на ньому не зберігаються взагалі. Це має велике значення для збору доказів, оскільки вилучати комп'ютер, який зберігає дані на хмарі, немає ніякого сенсу.

Крім того, менш відомим є те, що по технічним та комерційним причинам дані користувача можуть копіювати та зберігати одночасно в різних місцях, дані можуть перенаправлятись із одного місця до іншого в автоматичному режимі, і навіть один файл

[10] https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0
[11] Source: www.setecinvestigations.com/resources/techhints/Pages_per_Gigabyte.pdf

може бути розподілено і збережено в різних місцях. Все це приводить до складнощів у вилученні таких даних. Яку юрисдикцію застосовувати? Куди направляти запит на міжнародну допомогу?

Одна спроба розібратись у цій ситуації була зроблена у випадку Yahoo (Бельгія), де прокурор отримав в суді санкцію на доступ до емейл акаунтів. Yahoo(Бельгія) відмовилось виконувати судове рішення, зазначивши, що запит треба направляти до штаб квартири в США. Проте, Бельгійський прокурор успішно оскаржив таке рішення у Верховному Суді, що Yahoo (Бельгія) мало достатню присутність у Бельгії для застосування щодо компанії національного законодавства. В результаті компанію оштрафували і примусили надати запитувану інформацію.

4.8 Нулі та одиниці

У фізичному світі докази складаються з атомів та молекул, з яких далі формуються складні об'єкти.

Що стосується електронних доказів, всі вони є певними послідовностями базової одиниці комп'ютерної пам'яті – біта. Природа біта є бінарною, або двійковою. Це означає, що біт може бути або одиницею, або нулем.

На базовому рівні комп'ютер розуміє тільки двійкові цифри, або біти.

У випадку одного біта все просто, він є або нулем, або одиницею.

Але якщо додати ще один, другий біт, можна скласти 4 комбінації:

00

11

01

10

Додавання третього біта дає 8 комбінацій:

000

111

100

010

101

001

110

011

Четвертий біт ще раз подвоїть кількість комбінацій до 16 і так далі.

Саме тому комп'ютерна пам'ять прив'язана до ступенів двійки:

4, 16, 32, 64, 128, 512, 1024

І саме цьому в кілобайті 1024 байти, а не 1000.

Комп'ютер думає тільки цифрами, і ці цифри виражені у двійковій системі числення, але ми, люди, використовуємо десяткову систему. Коли ми рахуємо 1, 2, 3, 4, 5, 6, 7, 8, 9 і доходимо до 10, ми записуємо одиницю в колонку «десятки» та нуль в колонку «одиниці».

Десятки	Одиниці
1	0

Але комп'ютер, використовуючи двійкову систему, оцінює 10 як двійку. В десятковій системі 1001 є однією тисячею одним. А скільки це у двійковій системі?

Десяткова

1000	100	10	1
1	0	0	1

Одна тисяча один

Двійкова

8	4	2	1
1	0	0	1

1001 у двійковій системі = ? у десятковій?

(Відповідь внизу)[12]

Для запису у двійковій системі необхідно значно більше місця.

Переведення цифр у букви:
Зазвичай, говорячи про комп'ютерну пам'ять, ми використовуємо термін «байт». Байт складається з 8 бітів. Один байт є найменшою категорією у двійковій системі, що може представляти букву. Оскільки комп'ютер користується двійковою системою числення, йому необхідно переводити букви в цифри, і навпаки.

Існують різні системи такого перекладу. Найбільш поширеною є Американський Стандартний Код Обміну Інформацією (American Standard Code of Information Interchange (ASCII)). Ця система є фактично таблицею, в якій букви, цифри та спеціальні знаки представлені у вигляді двійкового коду. Це дозволяє нам перетворювати біти в комп'ютерній пам'яті у текст, який ми можемо читати.

Отже, комп'ютер бачить:

0100111001100001011101000110100101101111011011100110000101101100001000000101001101100011011010000110111101101111011011000010000001101111011001100010000001001010011101010110010000110011101100101011100 11

Ми можемо розбити цю послідовність на групи по 8 бітів (тобто на байти) наступним чином:

[12] 1001 у двійковій= 8+1 у десятковій = 9

01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 00100000 01010011 01100011 01101000 01101111 01101111 01101100 00100000 01101111 01100110 00100000 01001010 01110101 01100100 01100111 01100101 01110011

Далі ми переводимо ці байти в текст за допомогою ASCII та бачимо:

National School of Judges

Таким чином байт 01001110 означає 'N' байт 01100001 'a' і так далі. Навіть пробіли необхідно позначати байтом, оскільки для комп'ютера це просто символ.

Ви можете скористуватись такими конвертерами за наступними посиланнями.

https://www.rapidtables.com/convert/number/ascii-to-binary.html

https://www.binaryhexconverter.com/ascii-text-to-binary-converter

Система ASCII є дуже зручною, оскільки передбачає можливість вираження літер та символів лише одним байтом. На жаль, у випадку деяких мов, в тому числі української, для вираження літер використовується більше байтів. У випадку української мови необхідно 3 байти для однією літери. Найбільш поширена система називається Unicode.

Таким чином, на базовому рівні комп'ютерна пам'ять є просто послідовністю нулів та одиниць. Яким саме чином це реалізовано з технічної точки зору ми більш детально розглянемо згодом.

4.9 Мережі

Зараз не часто можна побачити комп'ютер без підключення до мережі.

Мережею можна назвати два або більше комп'ютерних пристроїв, що з'єднані один з одним. Існує велика кількість мереж. Найбільша і найвідоміша - Інтернет, але ви також зустрінете мережі з такими назвами, залежно від розміру та розташування мережі:

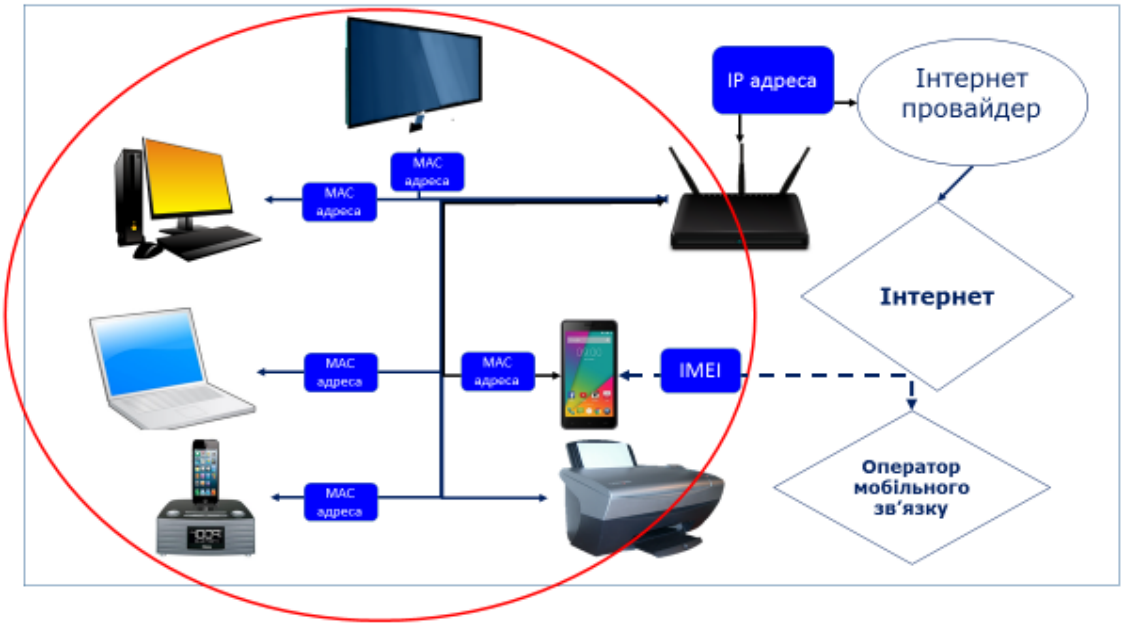
1) LAN – локальна мережа

2) WLAN – мережа безпровідної зони

3) WAN – широка мережа

Це основні види мереж, але існують і інші мережі, наприклад, мережа гуртожитку або мережа метро, які об'єднують пристрої в цих зонах.

Типова мережа зазвичай включає в себе декілька комп'ютерів, ноутбуків, планшетів. Ці пристрої будуть індивідуально з'єднані з модемом/ маршрутизатором, який є елементом мережі, і слугує точкою входу до мережі Інтернет. Мережа також може включати БФП (Багатофункціональний пристрій), смарт ТВ та безпровідні колонки. Смартфони, які використовують члени сім'ї, також, зазвичай, підключаються до мережі.



У випадку офісної мережі різниця буде у масштабі, а також можуть бути наявні спеціальні сервери, які знаходяться в спеціальній (серверній) кімнаті.

Як вже зазначалось раніше, точка входу до Інтернету - маршрутизатор. Коли маршрутизатор з'єднується з інтернет провайдером (компанія, яка надає інтернет послугу), йому присвоюється IP (Internet Protocol) адреса. Ми детальніше розглянемо IP адреси у наступній лекції. Простіше кажучи, IP адреса схожа на номер будинку на вулиці, який можна побачити, і який є публічною інформацією.

Різні пристрої у мережі мають також MAC (Media Access Control) адресу. Така адреса є унікальною; вона «прошивається» у пристрої виробником. За допомогою цієї адреси можна розпізнати пристрої у мережі. Маршрутизатор встановлює внутрішні з'єднання, спираючись на MAC адреси таким чином, щоб повідомлення завжди доставлялись правильному пристрою. Певна MAC адреса може бути в мережі тільки одна, і, зазвичай, MAC адреси не передаються поза внутрішню мережу.

Маршрутизатор керує вхідними та вихідними повідомленнями з інтернетом, а також зачасту він містить Брандмауер (Firewall), який перевіряє повідомлення на ризиковані або небажані передачі і блокує їх. Брандмауер може бути або програмним забезпеченням, або апаратним модулем.

Як Ви бачите, маршрутизатор в цьому випадку надає IP адресу і стає точкою доступу до мережі Інтернет. Маршрутизатор скеровує внутрішній трафік за допомогою MAC адрес. Далі маршрутизатор через Вашого інтернет провайдера надає Вам доступ безпосередньо до Інтернету. Окремо слід відмітити, що якщо мобільний пристрій (зазвичай телефон або планшет з сім картою) використовує стільникові дані замість Wi-Fi, то в нього буде інша IP адреса, і він підключається за допомогою оператора мобільного зв'язку, а не провайдера.

Також слід зазначити номери IMEI (International Mobile Equipment Identity, тобто Міжнародні Ідентифікатори Мобільного Обладнання). IMEI адреси подібні до MAC адрес,

але використовуються, щоб ідентифікувати мобільний телефон у мережі передачі даних. Вони жодним чином не пов’язані із Сім карткою, і є властивістю саме телефону.

Отже, за допомогою інтернет провайдера можна відстежити мережу за допомогою IP адреси, а потім за допомогою MAC адреси можна відстежити конкретний пристрій в цій мережі. Аналогічно можна визначити і телефон за допомогою провайдера телефонних послуг.

Але не все так просто. IP адресу можна замаскувати або приховати за допомогою proxy (проксі) сервера. Proxy сервери - комп'ютери в інтернеті, які стають посередником. Як тільки пристрій з'єднується з proxy сервером, він стає точкою доступу до інтернету для цього пристрою. Будь-яка діяльність, що проводиться цим комп'ютером в інтернеті матиме IP адресу proxy сервера.

Є також Віртуальні Приватні Мережі (VPN), які подібні до proxy серверів, але комунікація з пристроєм також кодується. VPN також приховує або маскує істинну адресу IP.

Так, Указом Президента України № 133/2017 «Про введення в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» заблоковано доступ до деяких сайтів. Подібні заборони існують в деяких країнах щодо певних сайтів. Такі заборони можна обходити використовуючи проксі, або VPN. Проксі сервери змінюють IP адресу користувача на свою. При використанні проксі сервера, який розташований в іншій державі, в якій не заборонено доступ до сайту, можна отримати такий доступ. Крім того, використання проксі та VPN є ефективним засобом забезпечення безпеки ПК. При підключенні до сайту напряму, сайту надається IP адреса, і, використовуючи цю адресу, комп'ютер користувача можуть зламати, запустити вірус або вкрасти особисті дані.

При використанні проксі, він змінить IP-адресу користувача на свою, і зловмисник намагатиметься зламати не її, а проксі, який краще захищений.

Використання VPN є ще ефективнішим. Він працює фактично так само, як і проксі, але шифрує весь трафік, і Ваш інтернет провайдер бачить лише те, що користувач з’єднався з сайтом, який надає VPN послуги, і обмінюється з ним даними. Зміст цих даних є зашифрованим, і просте отримання доступу до них не має ніякого сенсу.

MAC адресу пристрою можна тимчасово змінити за допомогою спеціальної програми. IMEI також може бути змінений, але це досить складно. Врешті-решт, для приховання протиправної дії злочинцю простіше буде придбати дешевий телефон та потім викинути його.

Отже, незважаючи на наявність ідентифікаторів, таких як IP адреса, MAC та IMEI адреси, які залишають сліди, такі сліди можуть бути ненадійними, якщо злочинець володіє певними технічними знаннями.

5 МЕРЕЖА ІНТЕРНЕТ: ПРИНЦИПИ ФУНКЦІОНУВАННЯ

Мета навчання:

Слухачі знатимуть основні принципи роботи інтернету та засоби ідентифікування конкретних осіб.

Зміст:

1) що таке www
2) як ідентифікувати винного
3) категорії даних
4) протоколи та їх функція
5) MAC адреси та номери IMEI як ідентифікатори
6) Proxy сервери та VPN
7) хмара
8) засоби анонімізації та Darknet

5.1 Кількість користувачів

Інтернет - глобальна мережа з'єднаних комп'ютерів, яка об'єднує більш ніж половину світу. Згідно з internetworldstats.com, станом на кінець 2017 року 4 156 932 140 осіб (тобто 54.4% глобального населення) були користувачами Інтернету. З початку століття ця кількість зросла на 1 052%.

Згідно з даними Інтернет асоціації України, проникнення інтернету в життя українців збільшується щороку, і станом на друге півріччя 2018 року становить 65%.[13]

Згідно з дослідженням Wearesocial та Hootsuite, проникнення інтернету в різних регіонах світу у 2018 році виглядає наступним чином (слайд): https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338[14]

5.2 Складові мережі Інтернет

Незважаючи на загальне використання, Інтернет – це не всесвітня павутина (WWW). Інтернет складається з трьох основних складових: www (всесвітня павутина), глибока павутина та темна павутина. Ніхто не знає наскільки великим є інтернет. У 2010 році була проведена оцінка, згідно з якою в інтернеті міститься більше ніж 5 мільйонів Тб (1Тб це 1000 Гб), з яких тільки 0.04% індексував Google.

Поверхнева павутина є громадським інтернетом і складає приблизно 5% всієї павутини.

[13] https://inau.ua/sites/default/files/file/1806/ui_factum_group_ii_kvartal_2018.pdf
[14] https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338

Глибока павутина, з іншого боку, складається з приватних мереж, що належать урядам, офісних внутрішніх мереж, та корпорацій, таких як банки. Для доступу до таких мереж потрібні спеціальні ключі, і їх не індексують механізми пошуку, такі як Google або Bing.

Темна мережа (Darknet) – зашифрована частина Глибокої павутини, яку зайняли люди, що надають приховані і часто нелегальні послуги. Вони включають секретні чат кімнати (сайти для спілкування), незаконні роздрібні ринки, злочинні організації, але також і людей, які мають законні причини для переховування (як наприклад інакодумці).

5.3 Маршрутизація

Інтернет - ієрархічна структура із з'єднаннями між різними серверами, що діють подібно до шосе в глобальній дорожній мережі. Коли повідомлення посилається через Інтернет, воно спочатку розбивається на маленькі частини (під назвою 'Пакети') і кожен пакет самостійно обирає шлях до місця призначення. Як і в будь-якій дорожній мережі в інтернеті бувають пробки та затримки (подібно до скупчень транспорту або дорожніх робіт) тому використовуються спеціальні сервери під назвою маршрутизатори, які діють подібно до регулювальників руху транспорту і направляють пакети по оптимальним маршрутам. Оскільки ситуація постійно змінюється, пакети прямують різними маршрутами, де вони повторно збираються в єдине ціле. Якщо пакет, незважаючи на регулювальника - маршрутизатора, десь застряг або загубився, одержуючий пристрій розумітиме, що пакет відсутній і попрохає заміну. Звичайно, все відбувається майже миттєво.

Ви можете подивитись невелику відео лекцію як передаються пакети за адресою:

https://www.youtube.com/watch?v=sHHg-Ni3eIU

5.4 Категорії Даних:

Інформація на комп'ютерних пристроях зберігається в різних форматах Для найкращого розуміння в межах цього курсу можна виділити такі категорії.

Метадані

Метадані можна визначити як дані про властивості певних даних. Вони подібні до індексу або змісту в книзі. Вони містять дані, про що цей файл, його розмір, коли і ким файл був створений, коли востаннє редагувався, і так далі. Коли слідчий суддя надає доступ до інформації щодо дзвінків абонента – це є приклад доступу до метаданих, оскільки зміст розмов та повідомлень при цьому не розголошується, а надається лише інформація щодо того, кому вони адресовані, їх тривалість тощо.

Інформація про трафік (рух даних)

Ця категорія даних описує, як повідомлення було надіслане: адреси відправлення та призначення; час відправки; сервери, через які воно пройшло, та який було використано протокол.

Змістовні дані

Найвищий і найскладніша категорія даних – змістовні дані. Змістовні дані - це безпосередньо текст повідомлення чи інша інформація, яка передавалась, наприклад, фото чи відеофайл; такі дані є безпосереднім предметом комунікації. Це найчутливіша категорія, тому що будь-яке перехоплення таких даних є порушенням конфіденційності і втручанням в особисте життя. Саме тому отримати дозвіл на доступ до такої інформації (наприклад зняття інформації з каналів зв'язку) дуже важко, але такі докази є найкращими при доведенні певних фактів та обставин. Цей тип даних подібний до листа всередині конверту. Досить просто побачити конверт, марку поштового відділення і найменування відправника та адресата, але щоб прочитати текст листа необхідно отримати спеціальний дозвіл.

При цьому, не завжди Вам потрібні змістовні дані для доказування певних обставин. Досить часто можна зробити певні висновки просто аналізуючи телефонні метадані.

5.5 URL (Єдина вказівка ресурсу)

Більшість людей назвало б URL адресою сайту чи доменним ім'ям. Як ми вже побачили, кожне підключення до Інтернету має IP адресу, але такі номери набагато складніше пам'ятати, ніж слова, тому ми використовуємо URL. Хоча ми можемо вставити IP адресу в поле адреси в браузері замість URL, більшість з нас вважає за краще написати назву сайту. Комп'ютер, проте, все одно перетворить URL на IP адресу, тому що комп'ютерам зручніше використати числа. Це здійснюється через (DNS) Системи Доменних Імен, які автоматично здійснюють заміну адреси на IP адресу.

Ви вводите назву потрібного сайту в адресному рядку браузера, який потім запитує IP адресу сервера з цією назвою у DNS. Уже за отриманим IP встановлюється з`єднання і починає відбуватися обмін інформацією між пристроями.

URL (адреса сайту) Національної Школи Суддів є

http://www.nsj.gov.ua

Але якщо ви введете наступну IP адресу у ваш браузер, ви потрапите туди ж:

83.218.242.227

URL має містити достатню інформацію про географічне положення сервера, щоб ідентифікувати пункт призначення.

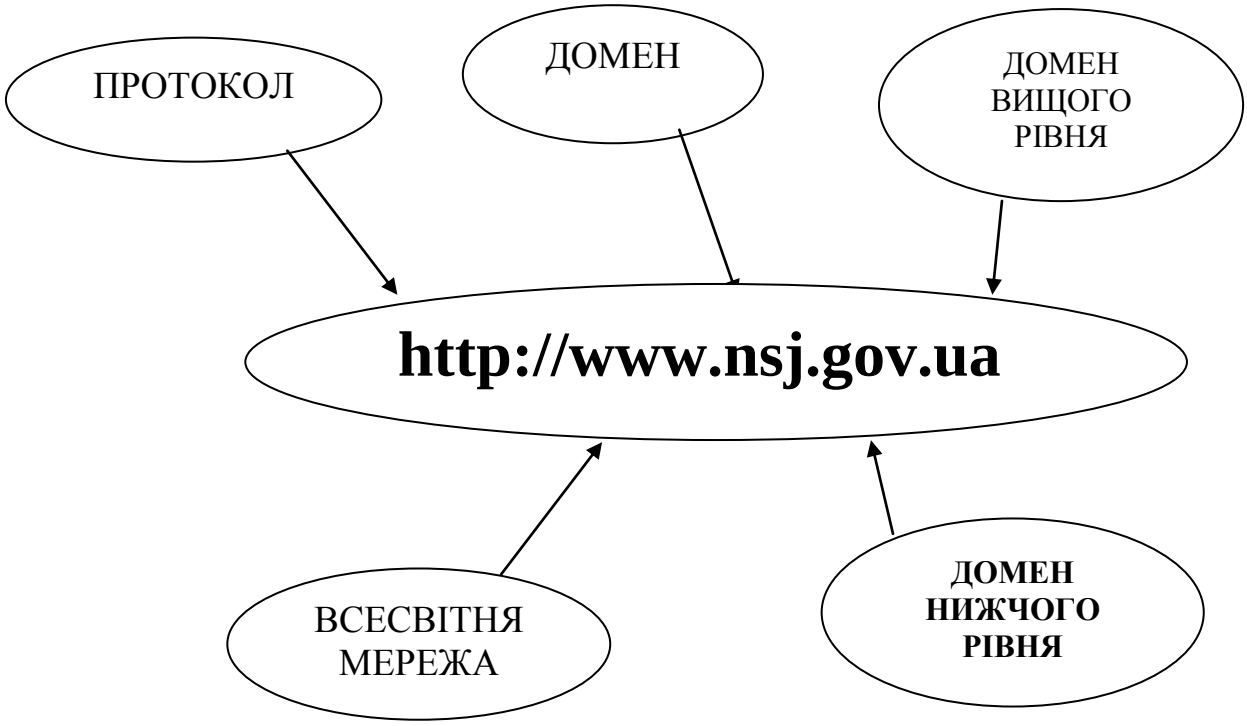
Перша частина, що стоїть перед :// роздільником, вказує використаний протокол. Http показує, що вебсайт використовує протоколом передачі гіпертекстових файлів.

Наступна секція www підтверджує, що адреса знаходиться у всесвітній павутині.

Потім стоїть безпосередній домен. Тут це - nsj. Це найбільш унікальна частина адреси.

Gov вказує, що це область, яка знаходиться у власності уряду. Це піддомен, або домен другого рівня.

Ua – домен першого рівня, найвищий рівень в ієрархії системи доменного імені, і в цьому URL він вказує Україну.



Як вже було зазначено, існує домен кореневого (першого) рівня, який позначається крапкою . Наступний рівень ієрархії — це домени наступного рівня. Вся структура служби DNS є ієрархічною. Існують домени першого, другого, третього, n-го рівнів.

Розглянемо доменне ім'я комп'ютера department.firma.isp.ua. Тут доменом першого рівня є ua, другого — isp, третього — firma, і четвертого — department.

Щоб простіше зрозуміти, як працюють різні доменні рівні, їх можна порівняти із поштовою адресою. Домен першого рівня – країна в адресі, домен другого рівня – це щось на кшталт області або міста, і так далі.

Усі IP адреси і доменні імена призначає неприбуткова організація в США Корпорація з Управління Доменними Іменами та IP адресами (ICANN). Вона формує політику роботи (наприклад, дозволені домени першого рівня) і управляє базами даних різних доменних імен.

В адресі www.nsj.gov.ua домен першого рівня вказує на країну, але є багато різних доменів першого рівня. Деякі не вказують на країну, а вказують на вид діяльності: .com означає комерційне підприємство; .gov - урядовий орган; .org – організацію. Майже всі країни зараз мають домен першого рівня, але існують багато інших доменів першого рівня. Деякі домени становлять несподіваний інтерес для комерційний сайтів через привабливе найменування, наприклад: .me для Чорногорії, .my для Малайзії та .tv для Тувалу.

Організація	Країна	Інший
.gov	.ua	.biz
.org	.uk	.io
.int	.y	.news

.com	.de	.rocks
	.eu	.social

5.6 IP адреси

Як вже зазначалось раніше, IP адресу можна відстежити до конкретного пристрою.

Є два види IP адрес: IPv4 і IPv6.

IPv4:

Адреса формату IPv4 створена ще у 1983 році, і на теперішній час вона є найпоширенішою.

IP адреса є 32 бітним числом. Зручною формою запису IP адреси формату IPv4 є запис у виді чотирьох десяткових чисел від 0 до 255, розділених крапками.

Це IPv4 адреса Національної школи суддів:

83.218.242.227

Максимальне число перестановок цього IPv4 формату складає 4 294 967 296, але раніше в сесії ми бачили, що зараз вже існує 4 156 932 140 користувачів інтернету і усім їм потрібна адреса IP, щоб з'єднатися з Інтернетом.

IPv6:

Кількість 4,3 мільярда - це дуже велике число, але його недостатньо для задоволення зростаючих потреб населення в підключених до інтернету пристроїв, таких як ноутбуки, планшети, смартфони. Тому був створений протокол IPv6. Він використовує адресний простір розміром 128 біт. Тому загальна кількість адрес буде 2 в 128 ступені, а цього нам вистачить на багато десятиліть, а, можливо, і століть. Адреса розміром 128 біт відрізняється від адреси IPv4. Кожна група поділяється двокрапкою замість крапки і складається з 16 біт, у вигляді чотирьох шістнадцятирічних цифр.

Безсумнівно, IPv6 краще свого попередника, але у нього немає зворотної сумісності з IPv4, і це його головний недолік. І тому всі пристрої повинні підтримувати ipv4 і ipv6, поки весь інтернет повністю не перейде на останній. Незважаючи на те, що IPv6 існує вже більше 10-ти років, його розгортання так і не набрало обертів, навіть з огляду на те, що адресний простір закінчується.

IPv4 використовується приблизно у 99% підключень до мережі інтернет станом на теперішній час.

5.7 Шістнадцяткова система числення

Шістнадцяткова система числення — це позиційна система числення з основою 16. Кожне число в ній записується за допомогою 16-ти символів. Арабські цифри від *0* до *9* відповідають значенням від нуля до дев'яти, а 6 літер *A*, *B*, *C*, *D*, *E*, *F* відповідають значенням

від десяти до п'ятнадцяти. Шістнадцяткова система числення широко використовується у програмуванні, оскільки кожна шістнадцяткова цифра представляється чотирма бінарними цифрами (бітами), і основне застосування шістнадцяткового запису — це зручний запис двійкового коду.

Існують спеціальні конвертери для переведення чисел із однієї системи числення до іншої, наприклад:

https://www.binaryhexconverter.com/decimal-to-hex-converter

https://fin-calc.org.ua/ua/calculator/conversion/notation/any/

5.8 Статична та динамічна IP адреси

Статична IP адреса задається користувачем у налаштуваннях пристрою, або надається автоматично при підключенні пристрою до мережі та не може бути присвоєна іншому пристрою.

Динамічна IP адреса надається автоматично при підключенні пристрою до мережі і використовується протягом обмеженого проміжку часу, зазначеного в службі, яка надала IP адресу.

Статична адреса використовується у разі потреби постійного підключення до мережі. Враховуючи, що більшість із нас не потребує постійного підключення, а також те, що протокол IPv4 має обмеження щодо кількості можливих адрес, більшості пристроїв надається динамічна адреса. Тобто інтернет провайдер при підключенні надає певну адресу пристрою, і ця адреса застосовується увесь час дії одного підключення. Як тільки підключення закінчується, ця адреса стає доступною для надання іншому пристрою. Звичайно, провайдер має дані, хто, коли і де користувався пристроями, але із цього випливає, що будь-який запит інформації повинен містити чіткі часові межі з точністю до секунди для того, щоб отримати правильні дані.

5.9 Whois

Ніхто фактично не володіє доменним ім'ям. Доменні імена тільки орендуються за винагороду на певний період. Відомості про орендаря зберігаються в спеціальному реєстрі, який утримується ICANN. Для з’ясування цих даних та іншої практичної інформації про домен можна використати сервіс WHOIS.

Ці дані вважались публічними, і доступ до них був відкритий, що дозволяло побачити ім’я та адресу орендаря. Але зараз за додаткову плату компанія може підміняти ім’я (назву) та адресу реєстрації, що дозволяє залишатись анонімним.

Але на сьогодні така послуга може стати застарілою. Після прийняття Загальних правил захисту даних Європейського Союзу триває дискусія щодо того, чи є загальний публічний доступ до даних Whois законним. Також слід відмітити, що зареєструвати домен із хибними даними досить просто.

Зазвичай ви зможете побачити:

- ім'я (назву) орендаря домену

- дату реєстрації
- дату закінчення оренди
- засоби зв’язку із адміністрацією сайту
- засоби зв’язку у разі виникнення технічних проблем
- сервери, які використовуються цим доменним ім'ям

Дані Whois можуть бути дуже корисними при ідентифікації власників чи орендарів сайту.

Сайти, які дозволяють використати сервіс Whois:

https://whois.icann.org/en

https://www.whois.com/whois

https://whois.domaintools.com/

5.10 Машина Wayback

Вебсайти регулярно оновляються, перероблюються та припиняються. Є некомерційний проект, який зберігає архів вебсайтів, починаючи з 1996 року. Машина Wayback робить знімки вебсайтів у всьому WWW просторі та слідкує за ними. Не усі вебсайти копіюються щодня, але деякі популярні вебсайти можуть копіюватись і частіше, ніж раз на день.

Сайт програми:

http://web.archive.org

Якщо вебсайт було копійовано (заархівовано), то Ви можете його продивитись в повному обсязі в тому вигляді, якій він мав на момент копіювання.

На слайді Ви можете побачити сайт відомого українського провайдера електронної пошти, який зберігався **11 484** разів з 2003 по 2018 рік. Це є дуже зручним способом перевірити, наприклад, зміст та сам факт розміщення певної інформації (статті, фото чи відео запису тощо) на сайті в певний період часу навіть після видалення такої інформації з сайту.

5.11 Відстеження IP адреси

Існують декілька сайтів, які дозволяють отримати відомості щодо IP адреси:

www.whatsmyip.org

www.whatismyipaddress.com

Такі сервіси надають Вам інформацію про певну IP адресу. При натисканні кнопки «надати більше інформації» Ви можете побачити більше, як то географічне розташування адреси, інтернет провайдер, координати та інше.

Маючи такі дані можна звертатись до провайдера із відповідним запитом, щоб з'ясувати, хто користувався адресою у певний час. На жаль, як ми вже обговорювали, при роботі з

електронними доказами слід пам'ятати, що існує багато способів приховати свої справжні дані.

Найпростіший спосіб сховатись - піти до громадського місця, в якому є безкоштовний wifi (наприклад публічна бібліотека, бар, аеропорт, спортзал тощо), і з'єднатись з інтернетом там. Таким чином, якщо хтось стежитиме за вашою адресою IP, він побачить саме це місце входу. Ульбріхт Росс, засновник і адміністратор першого незаконного сайту роздрібної торгівлі в Темній Мережі, щодо якого ухвалено вирок в США, був заарештований, сидячи в громадській бібліотеці під час користування громадським wifi.

Ми вже також зазначали про використання Proxy серверів, VPN (віртуальних приватних мереж).

Віртуальні приватні мережі можуть бути настільки ефективними у приховуванні особи користувача, що деякі країни забороняють їх використання або застосовують суворий контроль щодо їх використання.

Також слід відмітити архітектуру Carrier Grade NAT. Carrier Grade Network Address Translation (CG NAT). Це метод, якій може застосовувати інтернет провайдер для управління доступом користувачів до інтернету. При його застосуванні сотні користувачів можуть мати одну IP адресу на всіх, що значно ускладнює ідентифікацію конкретного пристрою.

Ми також вже згадували MAC адреси. Це унікальні номери, прошиті в пристрої виробником (прошиті в мережевій карті). Тому адреси MAC можуть також ідентифікувати виробника мережевої карти цього пристрою.

Зазвичай MAC адреса потрібна тільки в місцевій мережі. Це означає, що MAC адреса не передається за межі маршрутизатора/роутера/модема. Проте, MAC адреса кодуватиметься в IPv6 адресі (у разі використання такого формату адреси) і може бути вилучена з неї особою, яка володіє спеціальними знаннями. В такому випадку MAC адресу можна приховати тільки заздалегідь скориставшись спеціальним програмним забезпеченням.

Наявність MAC адреси є ефективним доказом того, який саме пристрій використовувався в інтернеті, але тільки якщо цей пристрій вже у Вас. Якщо його немає, то MAC адреса не допоможе Вам його знайти. Крім того, змінити MAC адресу досить просто.

5.12 Хмара

Для чого ви користуєтеся Хмарою?

Явище хмари набуло неймовірного розповсюдження за останні роки. Ви, мабуть, вже користуєтеся хмарою. Це означає, що всі дані, в тому числі дані програм, зберігаються десь поза пристроєм та внутрішньою мережею.

Приклади хмарних сервісів:

- Послуги електронної пошти як наприклад Gmail/Hotmail/Outlook
- Послуги зберігання як, наприклад, Dropbox, iCloud, OneDrive

- Програмне забезпечення, таке як AWS, Google Docs і Microsoft Office 350

По суті, хмара - віртуальний простір, в якому зберігаються дані та надаються комп'ютерні послуги.

Ми вже обговорювали особливості хмарного зберігання даних; повторимо ключові особливості:

- зберігається де завгодно у світі
- постійно переміщується
- дублюються більш ніж в одному місці
- розділяються та розподіляються по різним серверним фермам в різних місцях
- шифруються користувачем за допомогою потужного ключа шифрування таким чином, що навіть якщо ви отримаєте файл, без ключа його неможливо буде прочитати.

5.13 Програмне забезпечення для анонімізації

Найбільш поширене програмне забезпечення для анонімізації називається «Цибульний Маршрутизатор» або TOR. Цибульний Маршрутизатор був розроблений науково-дослідною лабораторією воєнно морського флоту США в 90-х роках минулого століття для того, щоб дозволити агентам під прикриттям та/або військовим посилати повідомлення через інтернет безпечно і анонімно. На сьогоднішній день TOR адмініструє група захисників приватності. TOR - важливий інструмент як для журналістів-розслідувачів, так і для політиків-дисидентів. Також, з очевидних причин, він є дуже корисним для злочинців.

Мережа TOR складається з сотень комп'ютерів у всьому світі, які надаються їх власниками-добровольцями для виділу частини ресурсів їх пристрою. Ці ресурси використовуються для отримання і передачі далі повідомлень в мережі TOR. Такі комп'ютери називаються «вузлами». Коли користувач приєднується до мережі TOR, він підключається до зашифрованої групи вузлів. Така група працює впродовж заданого за замовчуванням періоду у 10 хвилин, після чого створюється нове реле через інші вузли. Перед тим, як будь-яке повідомлення буде надіслано, воно багаторазово шифрується. Іншими словами, воно обгортається в захисні шари шифрування. Коли повідомлення проходить черговий вузол, черговий шар розшифровується (процес подібний до очищення цибулі). При проходженні останнього, вихідного, вузла знімається останній шар кодування і повідомлення повністю розшифровується і приходить до місця призначення у розшифрованому вигляді.

Домени темної мережі не можна знайти за допомогою звичайних браузерів, таких як Firefox, Chrome або Internet Explorer. Для цього необхідні спеціальні пошукові механізми (наприклад Duckduckgo, Torch або Onion URL Repository). URL адреси в темній мережі закінчуються на .onion (який не є доменом першого рівня в базі доменів ICANN).

Якщо хто-небудь хоче зайти до темної мережі, йому треба користуватися Браузером TOR. Це безкоштовне програмне забезпечення, яке може бути завантажене з Інтернету.

Темні Мережеві області надають широкий ряд послуг, у тому числі чат-кімнати, магазини, банківські послуги, особисті послуги, блоги. Види послуг та доступної інформації є подібними до тих, що Ви можете знайти на WWW. Різниця полягає в тому, що майже всі сайти темної мережі стосуються кримінальної чи іншої незаконної діяльності. Але може використовуватись і для прикриття законної діяльності, наприклад зустрічей журналіста та його таємного джерела.

6 ТЕЛЕФОНИ ЯК ДОКАЗ

Мета навчання:

У цій главі ви дізнаєтесь про деякі методи, за допомогою яких можна визначити місцезнаходження телефонів.

6.1 Телефонна залежність

Чи є у вас смартфон? Приз за перший смартфон[15] отримує модель IBM Simon, що надійшла до продажу 1994 року, але «ера смартфонів» по-справжньому розпочалася 2007 року з появою iPhone від Apple. За останнє десятиліття зростання впливу смартфонів було приголомшливим. За деякими оцінками, 92% населення України володіє мобільними телефонами, а 41% – смартфонами.[16] Це означає, що понад 90% населення добровільно має при собі потенційний пристрій стеження.

Смартфони стали невіддільним аксесуаром сучасного життя. Під час нещодавнього дослідження, проведеного у Великій Британії, було встановлено, що люди щодня в середньому витрачають 2 години 28 хвилин на свої смартфони (і цей показник підвищується до 3 годин 14 хвилин у віковій групі від 18 до 24 років). Крім того, дослідження також встановило, що смартфони перевіряють кожні 12 хвилин у години неспання, вони становлять найважливіші пристрої для доступу до Інтернету для 72% дорослих, а 71% ніколи не вимикає своїх смартфонів.[17]

Навіть якщо ці статистичні дані не відповідають реальному стану речей в Україні, вони очевидно демонструють, яку цінність може становити смартфон у плані доказів. У цій главі ми розглянемо, зокрема, те, як можна визначати місцезнаходження телефонів або відстежувати їх.

Сьогодні це може виглядати як кам'яний вік, але до настання епохи мобільного зв'язку кожен телефонний апарат мав свого фіксованого абонента, розташованого за фіксованою адресою, до якої було підведено стаціонарну лінію. Відстежити виклик можна було лише в режимі реального часу за допомогою спеціального устаткування, і якщо підозрюваний занадто рано клав слухавку, то зв'язок розривався й відстежити виклик виявлялося неможливим. Все стало набагато простіше, коли в цифрових дзвінках почали реєструвати номер абонента.

В інформаційну епоху телефони стали «мобільні» в найширшому сенсі цього слова. Мобільні телефони зменшились у розмірах від автомобільного акумулятора до тонкої фоторамки. Смартфони можуть все: фотографувати, відтворювати музику, відправляти електронну пошту, показувати телевізійні програми в режимі реального часу, здійснювати навігацію в Інтернеті. Іноді їх навіть використовують, щоб кудись подзвонити.

З роками розвиток технології пройшов декілька поколінь. Можливості телефонів 2G (другого покоління) були обмежені телефонними дзвінками та текстовими повідомленнями, що використовують технологію, доступну з початку 90-х років. Технологія 2G здатна працювати на швидкостях до 64 Кбіт/с (кілобіт за секунду) і потребує потужного цифрового сигналу. Їй на зміну прийшла технологія 3G, яка стала стандартом,

[15] Перший комерційний мобільний телефон – Motorola DynaTAC 8000X – надійшов у продаж 1983 року за ціною майже 4000 дол. США і важив 0,91 кг.

[16] https://www.statista.com/statistics/362800/electronic-device-usage-ukraine

[17] https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/decade-of-digital-dependency

що дозволив з успіхом користуватися смартфонами. Завдяки своїй поліпшеній пропускній здатності та швидкості передачі даних, 3G можна використовувати для відео, потокового ТБ, ігор і високошвидкісної навігації в Інтернеті. 4G є поточним стандартом і дозволяє розвивати швидкість до 1 Гбіт/с, що, у свою чергу, підтримує високоякісні застосунки. Сьогодні триває розроблення технології п'ятого покоління (5G). Це уможливить підвищену якість і розширені функції, обіцяючи «новий великий поштовх» застосункам для смартфонів.

Незалежно від покоління технології, мобільним телефонам потрібно під'єднуватися до бездротової антени або базової станції. Базові станції або вежі встановлюють з метою забезпечити найкраще покриття, можливе з погляду економіки. Більш густонаселені райони обслуговуватимуться значно більшою кількістю базових станцій, ніж за межами міста, і їхні сигнали часто перекриватимуться, так що деякі місця покриватимуться двома чи більше вежами, або «стільниками».

Велика різниця між стаціонарним телефонним зв'язком і мережею мобільних телефонів полягає в тому, що для того, щоб залишитися анонімним у мережі фіксованого зв'язку, підозрюваному треба скористатися таксофоном. Однак сьогодні можна придбати дешеві та одноразові мобільні телефони з передоплатою послуг, які не потребують реєстрації та які неможливо відстежити. Утім, ідентифікувати покупця такого телефону все ж таки можливо, знайшовши магазин, що продав пристрій (за номером IMEI), і переглянувши записи камер відеоспостереження в магазині та, де це доречно, перевіривши рух коштів на банківській картці.

Ми вже обговорювали номер IMEI (International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання), вбудований в телефон виробником.[18] Мобільні телефони з двома SIM-картами мають два різні IMEI – по одному на кожну SIM-карту. Номер IMEI реєструється під час першого під'єднання телефону до телефонної мережі. IMEI телефона можна переглянути, ввівши комбінацію *#06#.

6.2 SIM

SIM-карта (Subscriber Identity Module – модуль ідентифікації абонента) – це невелика мікросхема, вставлена в телефон, яка ідентифікує обліковий запис для постачальника телекомунікаційних послуг. Пам'ять SIM-карти невелика, але вона може містити корисну інформацію, зокрема історію дзвінків, список контактів і текстові повідомлення. Одним із нещодавніх нововведень в деяких SIM-картах став так званий «безпечний елемент» (Secure Element), який надійно зберігає особисті та фінансові дані та дозволяє телефону виконувати роль платіжного пристрою. Хоча «безпечний елемент» можна знайти в SIM-карті, він також існує у вигляді окремої вбудованої в телефон мікросхеми.

Важливо також пам'ятати, що SIM-карти можна замінювати або встановлювати в інші телефони (у цьому разі телефон вже не буде пов'язаний з тим же номером IMEI у мережі).

6.3 Обсяг пам'яті

Універсальність смартфона неможливо переоцінити. Пам'ять телефону (яку часто можна розширити, встановивши додаткову карту пам'яті) може містити текст, зображення, відео, дані календаря та звукові записи, а також дані застосунків, наприклад, WhatsApp, месенджера Facebook, Snapchat, Telegram чи Instagram. Це стало можливим не лише

[18] Ту ж саму функцію виконує ідентифікатор мобільного обладнання (Mobile Equipment Identifier – MEID).

завдяки стандарту 4G, а й нині доступним можливостям запам'ятовувальних пристроїв. Телефон з 64 ГБ пам'яті, навіть якщо 6 ГБ буде виділено під операційну систему, все ж таки матиме вільні 58 ГБ, які можна заповнити різними видами даних і застосунків. 58 ГБ достатньо для того, щоб 11 600 раз зберегти повне зібрання творів Шекспіра. З огляду на те, що деякі повідомлення можуть мати розмір лише в 10 байтів, це означає, що телефон може містити близько 5 800 000 повідомлень, у яких пошук за ключовими словами буде ускладнений. Це може становити значну проблему для фахівця цифрової криміналістики, який має перевірити телефон і гарантувати, що жодні дані, важливі для розслідування, не були втрачені.[19]

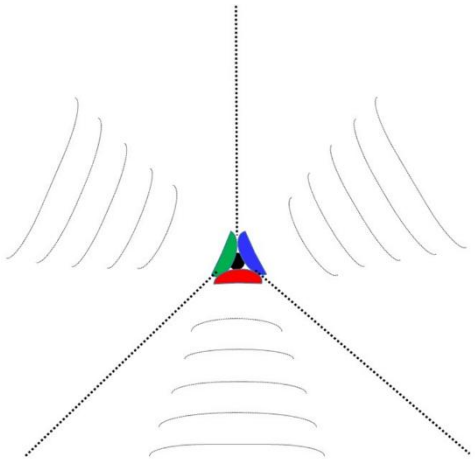
6.4 З'єднання

Навіть якщо телефон мобільний, він однаково має з'єднуватися з мережею, аби функціонувати. Коли телефон увімкнено, він автоматично шукає найсильніший сигнал від базової станції. Як правило (але не обов'язково), це буде найближча до нього антена. Щойно контакт встановлено, телефон і його номер IMEI реєструються на цій базовій станції (або вузлі стільникового зв'язку), і телефон залишатиметься під'єднаним до вежі, доки не натрапить на сильніший сигнал від іншого вузла, після чого від'єднається від першої базової станції та приєднається до другої. З переміщенням телефону з одного місця до іншого, він, відповідно, передаватиметься від одної до наступної базової станції в мережі.

Як вже згадувалося, найсильніший сигнал не обов'язково надходитиме від найближчої антени. З'єднання на вузлах стільникового зв'язку залежать від характеру місцевості, наявності будівель та інших суттєвих перешкод, висоти вежі та вихідної потужності передавача. Навіть той самий телефон у тому самому місці в різні дні може з'єднуватися з іншою вежею внаслідок погодних умов або поточного навантаження (тобто обсягу телефонного трафіку) на цій базовій станції.

Вежі базової станції можуть передавати всеспрямований сигнал (інакше кажучи, одночасно в усіх напрямках), але зазвичай на вежах встановлено декілька антен-«тарілок», що приймають і передають сигнал у певному напрямку. Наприклад, на базовій станції, обладнаній трьома «тарілками», кожна тарілка охоплюватиме сегмент у 120° навколо вежі.

[19] Блог «Verity Méchant», запис від 30 січня 2018 р. за адресою: https://encroaching.wordpress.com/



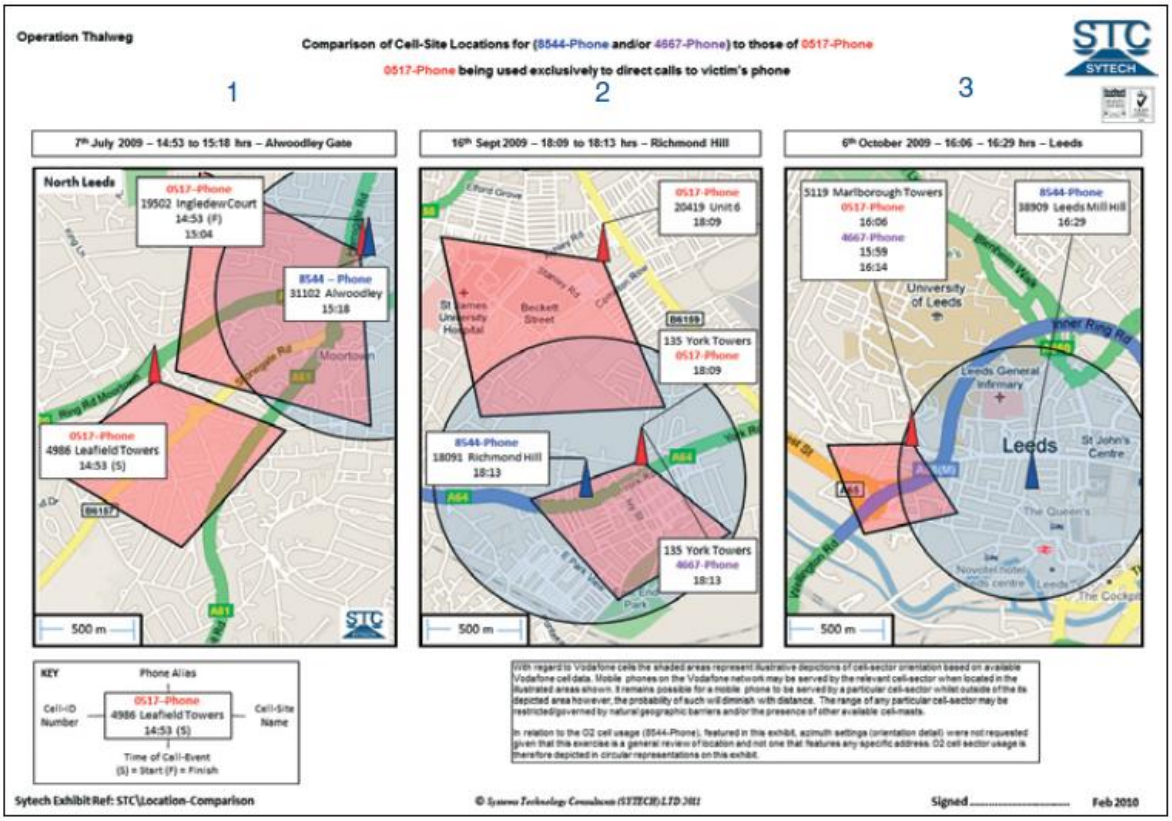
Під'єднання до однієї вежі на території міста, як правило, здійснюється в межах дільниці площею близько 1 кв. км. У сільській місцевості, де набагато менше базових станцій, один вузол стільникового зв'язку може охоплювати багато десятків квадратних кілометрів (телефон може з'єднуватися з вежею на відстані до 72 км).

Однак, тому що зони охоплення вузлами стільникового зв'язку в місті або міській місцевості часто перекриваються, телефон за короткий проміжок часу може з'єднуватися з різними базовими станціями. Телефони, що підтримують стандарти 3G і 4G, також можуть одночасно з'єднуватися з декількома стільниками, однак ці з'єднання не фіксуються в даних, що реєструються вузлом стільникового зв'язку. У записах буде видно лише те, що базова станція, з якою пристрій з'єднався на початку телефонного дзвінка, відрізняється від стільника, до якого пристрій був під'єднаний наприкінці телефонного дзвінка. У цьому разі місцеположення телефону можна оцінити точніше, аналізуючи, в якій саме точці сходяться сигнали від різних антен.

Фахівець також може оцінити відстань від телефону до базової станції, вимірюючи час проходження сигналу між вежею і телефоном. Це також може допомогти в уточненні його місцеположення.

Ось приклад того, як на практиці виявляють місцеположення, користуючись сигналом від вузлів стільникового зв'язку. Цей аналіз був виконаний британською компанією Sytech і відтворюється тут з її люб'язного дозволу.[20]

[20] Цей та інші приклади можна знайти в брошурі Sytech «Cell Site Analysis in Action: Successful Use for Evidential and Intelligence Purposes» (Практичний аналіз вузлів стільникового зв'язку: успішне використання з метою збирання доказів та інформації), доступній за адресою http://sytech-consultants.com/wp-content/uploads/2015/03/Sytech-Prosecution-Guide.pdf



6.5 GPS

Набагато точнішим методом визначення місцеположення телефону є система глобального позиціонування (Global Positioning System – GPS), в якій розташування телефону обчислюється стосовно групи супутників на геостаціонарній орбіті. Щоби скористатися цим методом, у телефоні має бути в наявності та активована функція GPS, а сам телефон має бути «видимий для супутника (що може виявитися складним серед міських будівель, які можуть блокувати сигнал). Як повідомляється, за хороших умов GPS може ідентифікувати місцеположення телефону з точністю 3-5 метрів, але в середньому точність становить 5-8 метрів. Це може залежати від низки чинників, включно з типом телефону, програмним забезпеченням і супутниковим охопленням, а також від характеру місцевості. Бетонні конструкції, дерева й навіть потоки повітря здатні викликати відбиття або перешкоди сигналу GPS, що робить результати менш надійними. Однак очікується поява нової технології, котра, як стверджують, забезпечує точність до 30 см.

Коли сигнал GPS зникає (наприклад, у разі втрати контакту зі супутником), телефон також зазвичай намагатиметься використати відкриті точки доступу WiFi та з'єднатися з вузлами стільникового зв'язку, щоб визначити місце свого розташування.

6.6 Перехоплювачі IMSI

Іншим способом визначити місцеположення мобільного телефону є перехоплювач міжнародного ідентифікатора користувача мобільного зв'язку (International Mobile Subscriber Identity – IMSI). Це активна технологія, що імітує роботу потужної базової станції, до якої б автоматично під'єднувалися мобільні телефони. Перехоплювач IMSI (відомий також як Stingray за назвою однієї з найпоширеніших моделей) після цього діє як

ретранслятор, дозволяючи звичайній мережі стільникового зв'язку забезпечувати нормальну роботу відповідного телефону. Це дозволяє здійснювати моніторинг даних, що проходять через телефон.

Визначення місцеположення телефону за допомогою перехоплювача IMSI здійснюється методом тріангуляції. Після того, як пристрій захопить сигнал телефону, на мапі позначають напрям до нього. Потім перехоплювач IMSI переміщують один чи більше разів, щоби зафіксувати додаткові напрями. Місце перетину напрямів на мапі означає місцеположення телефону.

Використання перехоплювачів IMSI становить таємницю, і детальної інформації про це небагато, але 2013 року було оголошено про початок випуску прихованих портативних перехоплювачів IMSI.[21] Як потужна, але дещо секретна технологія спостереження, перехоплювачі IMSI також є об'єктом уваги та занепокоєння з боку спостерігачів за дотриманням прав людини.[22]

Контрольні запитання:

1. До якої кількості вузлів стільникового зв'язку здатний одночасно під'єднуватися мобільний телефон?

2. Які нинішні показники точності, з якою визначають місцеположення за допомогою GPS?

3. Які фактори зовнішнього середовища впливають на сигнал від базової станції?

Вивчення та повторення:

Спробуйте порівняти способи визначення місцеположення мобільного телефону з і без GPS, наводячи переваги та недоліки кожного з них

[21] https://arstechnica.com/information-technology/2013/09/the-body-worn-imsi-catcher-for-all-your-covert-phone-snooping-needs/
[22] https://www.theinquirer.net/inquirer/news/3037243/privacy-international-challenges-brit-cops-use-of-intrusive-imsi-catchers

7 СУДОВА ЕКСПЕРТИЗА ЕЛЕКТРОННИХ ДОКАЗІВ

Мета навчання:

Надання учасникам практичної інформації щодо найкращої практики збирання електронних доказів та розуміння того, які небезпеки може спричинити недотримання порядку цілісності доказів.

7.1 Можливості цифрової криміналістики

Внесок, зроблений у науку розслідування експертним вивченням доказів, є величезним. Це сприяло підвищенню ефективності та надійності кримінального правосуддя шляхом надання нових об'єктивних способів перевірки фактів та виявлення деталей, непомітних неозброєному оку. Розвиток електронних пристроїв в інформаційну епоху означає, що всі злочини будуть містити елемент електронних доказів. Проте у випадку, якщо ці докази не будуть виявлені, вилучені та належним чином проаналізовані, це буде не тільки втратою можливості, але й призведе до порушення засад верховенства права. Більше того, ті, на кого покладено обов'язок зберігати та захищати інтереси правосуддя, повинні знати, принаймні, основні принципи, щоб відповідальним чином виконувати ці обов'язки. Їм потрібно вміти відповідати на складні питання і з упевненістю досліджувати докази, надані їм.

93% мешканців України мають доступ до Інтернету, а мобільних телефонів більше, ніж осіб, що живе в країні[23] – відтак ймовірність зустріти електронні докази є дуже високою. Найбільший виклик полягає у швидкості розвитку та змін, що впливають на обробку таких доказів. Найкраща практика сьогодні може бути безповоротно змінена в майбутньому завдяки новому відкриттю чи інноваціям.

7.2 Електронні докази у випадках корупції

Електронні докази у випадках корупції можуть передбачати:

- Спілкування між сторонами. Це може передбачати записи телефонних дзвінків, SMS, електронних листів, Voice Over IP (VOIP), таких як Skype або Google Hangouts, спілкування, що здійснюється в віртуальних середовищах онлайн-ігор. Електронні докази можуть, також, підтвердити, що зустрічі між сторонами відбувалися в реальному світі.

- Записи щодо будь-яких угод між сторонами або переговорів, які зберігаються в електронному вигляді на пристрої або в Інтернеті, електронній пошті або у виді цифрових записів, зроблених як «гарантії безпеки» однією стороною стосовно іншої;

- Докази багатства невстановленого походження, коли людина зі скромним доходом живе абсолютно не за власними доходам або придбала дорогі речі чи екстравагантним чином відпочиває. Докази можуть передбачати фотографії або

[23] Згідно з даними Вікіпедії, населення України становить 45579617 осіб, проте в країні налічується 57505555 мобільних телефонів. https://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use

публікації в соціальних мережах, чеки чи інші докази придбання розкішних товарів.[24]

- Підозрювана особа може здійснити запит або вжити заходів для приховування чи "відмивання" таких доходів. Ці дії можуть передбачати створення фіктивних компаній або офшорних установ чи інвестування у криптовалюту, що неможливо відстежити, чи інші фінансові інструменти. Особа може зробити це від власного імені або від імені близьких членів родини. Зараз дослідження таких можливостей здійснюється в Інтернеті, і будь-яке спілкування, яке буде відбуватися після дослідження, буде електронним.

- Існує також багато випадків, коли особи, що планували злочини, шукали в Інтернеті поради від інших про те, як краще його вчинити. Якщо така особа є не надто освічена в цифровій сфері, усі її дії або пошуки будуть фіксуватися.

7.3 На місці злочину

Всі стандартні запобіжні заходи застосовуються як для отримання електронних доказів, так і для отримання речових доказів. Ви повинні знайти докази, переконатися, що вони безпечні, та захистити їх від псування.

Чи існують в Україні стандартні процедури роботи? Стандартні процедури роботи або СПР (Standard Operating Procedures, SOP) є інструкцією для особи, яка повинна виконувати певну роботу, і може бути особливо корисним у такому складному занятті, як пошук та обробка електронних доказів. Процедури, також, надають судам стандарт, за яким можна вимірювати та оцінювати виконання такої роботи. З погляду фактичного змісту, СПР може дати вказівку пошуковій команді на те, що робити і в якому порядку; це може бути вказівкою щодо того, яке обладнання використовувати; як і де шукати певні типи пристроїв тощо. Враховуючи це, СПР ніколи не можуть передбачати всі можливі випадки, і, отже, вони повинні бути достатньо гнучкими та забезпечувати достатньо місця для винахідливості під час роботи слідчого або експерта-криміналіста. СПР встановлюють параметри, і якщо експерт вважає доречним вийти за межі цих параметрів, для відсутності запитань у суду, він повинен вміти пояснити, чому він так вчинив.

Будь-яка дія повинна бути чітко і повною мірою документована, як і на будь-якому місці злочину.

7.4 Активні пристрої

Якщо залучено активний пристрій, то перше, що потрібно зробити, – це переконатись, що будь-яка підозрювана особа не має доступу до пристрою (а також до будь-яких інших доказів). Якщо підозрювана особа, що має достатні кібер-знання, може мати доступ до активного пристрою, можуть статися певні небажані речі. Він/вона може:

- Завершити роботу комп'ютера, аби втратити будь-яку інформацію про роботу пристрою на той момент, а також будь-які активні підключення до хмарних сховищ;

- Встановити програму самовидалення, яка знищить усю інформацію;

[24] https://news.artnet.com/art-world/romania-finance-minister-bribed-renoi-282540

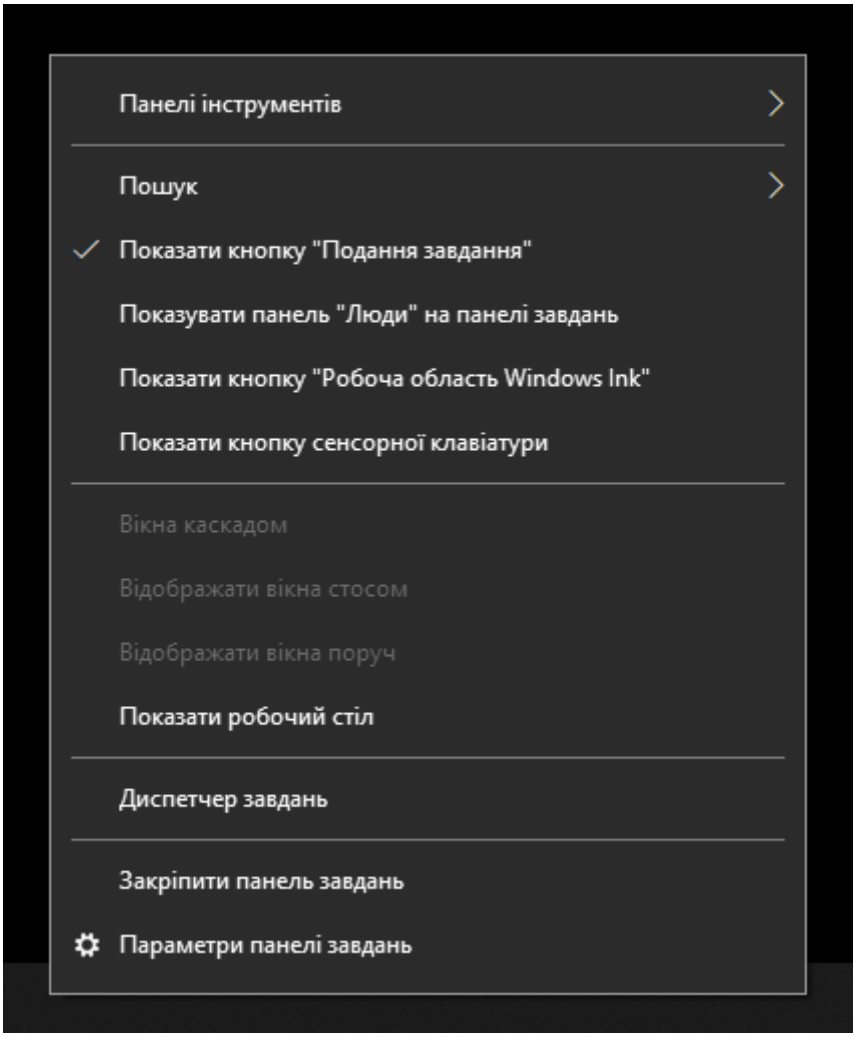
- Увімкнути шифрування;
- Повідомити інших співучасників.

Після того, як підозрюваного буде ізольовано від активного пристрою, правоохоронці повинні уважно стежити за тим, що відбувається на екрані (бажано з фотографіями чи відео) та створювати діаграми, що показують, як під'єднуються різні пристрої (це дасть змогу так само під'єднати пристрої пізніше в лабораторії).

Різні країни мають різні правила стосовно того, як правоохоронець може взаємодіяти з активним пристроєм. Чи може він рухати мишею, щоб переконатися, що комп'ютер перебуває в сплячому режимі? З іншого боку, чи може правоохоронець вводити команди до машини для завантаження інформації з підключення до Інтернету підозрюваного або для пошуку в оперативно-запам'ятовуючому пристрої (ОЗП)? Це питання, що вирішуються на національному рівні. Проте, коли машина все ще ввімкнена та під'єднана, існують певні можливості, які зникають після вимкнення пристрою.

Проблема полягає в тому, що на комп'ютері, який працює, багато процесів відбуваються в його короткостроковій пам'яті – оперативній пам'яті. У наші дні це цілком нормально для звичайного пристрою мати оперативну пам'ять 8 Гб. У наші дні її розмір для ігрових комп'ютерів, зазвичай, становить 8-32 Гб, а оперативна пам'ять у спеціалізованих пристроях може бути ще більшою (наприклад, для тих, які призначені для редагування медіа). Вся ця потенційна інформація буде втрачена під час знеструмлення. Після вимкнення, комп'ютер «втратить» усі незбережені документи та будь-який доступ до файлів або «послуг» у хмарних сховищах.

Якщо Ви використовуєте комп'ютер з ОС Windows (з Windows 10), клацніть правою кнопкою миші на порожній області панелі завдань у нижній частині екрана та в меню, що з'явиться, виділіть диспетчер завдань, а потім клацніть лівою кнопкою миші на цьому пункті.



Ви побачите, що відбуваються різноманітні процеси, про які Ви, як користувач, зазвичай, нічого, на щастя, не знаєте. Особливо погляньте на вкладки «Інформація» та «Послуги». Вони показують вам, що відбувається у фоновому режимі на вашому комп'ютері.

Незалежно від того, чи дозволяє законодавство України отримувати доступ до такої інформації чи ні, це дуже делікатне завдання, і його слід виконувати лише фахівцю, який був належним чином підготовлений та уповноважений це зробити. Кожна дія, кожна кнопка, натиснута на комп'ютері, дещо змінює його пам'ять, і у випадку, якщо це було зроблено невміло, ця дія може становити правову загрозу того, що докази стали недостовірними та неприйнятними.

Одним з важливих запобіжних заходів щодо цього є використання «writeblocker» – блокувальника запису. Він може набувати форми апаратного пристрою або програмного забезпечення, яке ефективно створює «клапан» одностороннього доступу, що дає змогу вивести інформацію з пристрою, але нічого не вводити в нього.

Окрім того, це не може повторюватися досить часто. Кожна дія повинна бути задокументована, щоб вона за потреби могла бути переглянута під час розслідування та судового процесу. Це особливо важливо, якщо було вжито заходів, які є, якимось чином, нестандартними. Якщо це можливо, причини для таких надзвичайних дій також повинні бути зафіксовані. Саме тому використання відео є настільки корисним.

Найважливішим з погляду документації є акт вилучення, в якому зафіксовано, коли, де і ким було вилучено кожен предмет. У ньому також реєструється все, що робиться з цим предметом після його вилучення, включно з до, під час і після судового розгляду.

Оскільки на місці злочину можуть зберігатися різні типи пристроїв, незалежно від факту залучення фахівця, його необхідно проінформувати заздалегідь про будь-які дані або інформацію про типи електронних доказів, які слід шукати, або які можуть бути наявними на місці злочину (включаючи, по можливості, типи операційної системи та марки обладнання). Це дасть змогу фахівцеві принести правильне обладнання та правильно здійснити усі необхідні процедури. Слід розуміти, що пристрій Windows сильно відрізняється від пристрою Android, Apple або Linux, а настільні комп'ютери і ноутбуки та смартфони передбачають різні криміналістичні вимоги до пристроїв.

Будь-яка кнопка, натиснута на комп'ютері, змінює його пам'ять і, отже, потенційно змінює і засмічує докази.

7.5 Неактивні пристрої

Як ми вже бачили, пристрої на місці злочину, які перебувають у вимкненому стані, вважаються неактивними, і саме вони становитимуть переважну більшість пристроїв, вилучених під час пошуку. Оскільки вони неактивні, вони можуть поступово досліджуватися у лабораторії.

Мобільні телефони можуть розглядатися як щось середнє між активним та неактивним пристроєм, оскільки вони зрідка вимикаються навіть попри те, що вони можуть і не використовуватися. Мобільні телефони постійно обмінюються даними з базовими станціями/антенами своїх телекомунікаційних провайдерів, а криміналістична експертиза мобільних телефонів є ще більш вимогливою для експертів цієї сфери. Проте існує обладнання, за допомогою якого практично будь-хто з мінімумом навичок може завантажити вміст пам'яті телефону (завжди припускаючи, що телефон не зашифровано, а акумулятор все ще має заряд). Юридично така дія може вимагати подальшого рішення від слідчого судді.[25]

За потреби, експерт-криміналіст повинен мати можливість здійснити «зміни почерговості» у процедурі відновлення доказів. Існують різні уявлення про те, чи повинні абсолютно всі пристрої, що можуть забезпечувати електронні докази, вилучатися з місця злочину, або ж це правило повинно застосовуватися лише до основних та очевидних пристроїв. З одного боку, існує ризик неврахування необхідних доказів, а з іншого боку, обсяг даних на стандартному місці злочину є настільки великим, що це може спричинити величезні затримки та додаткові витрати, спричинені звичайною обробкою та зберіганням будь-яких надмірних даних без будь-якої гарантії, що вони містять корисну інформацію. Звісно, рішення обумовлене не лише операційним контекстом, а й буде залежати від того, наскільки широкою була ухвала слідчого судді, а також того, що конкретно вона дозволяла вилучити.

[25] У Великобританії ордери не потрібні. Див. Privacy International (2018) Digital stop and search: how the UK police can secretly download everything from your mobile phone https://www.privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile

Окрім того, виникають інші юридичні та операційні питання: чи повинні оглядатися/вилучатися інші електронні пристрої, які використовуються в приміщенні (тобто не виключно підозрюваним)? Чи слід здійснювати вилучення приладів, які належать іншим членам сім'ї чи сусідам, якщо підозрюваний має доступ до них?

На ці питання остаточних відповідей немає. Багато чого буде залежати від фактів та конкретних обставин слідства (а також наданих законних підстав).

Ми вже розглянули джерела електронних доказів, але ці джерела не завжди можуть бути очевидними. Периферійні пристрої (пристрої, що приєднуються до комп'ютера або мережі) іноді можуть бути випущені з уваги, але, наприклад, більшість принтерів, сканерів та факсимільних апаратів зберігають електронні записи оброблених цими пристроями документів.

Пристрої або портативні носії інформації можуть бути добре прихованими. USB-флеш-накопичувачі та SD-карти можуть бути надзвичайно малими або замаскованими під повсякденні об'єкти, які можна легко пропустити. В одному випадку зовнішній жорсткий диск, що під'єднувався через безпровідну мережу, було вмонтовано у стіну (слідчі знали, що існують докази, і змогли знайти їх за допомогою скануючого Wi-Fi пристрою). Інакше кажучи, у випадку, коли підозрюваний є технічно освіченим, звичного підходу до обшуку навряд чи буде достатньо, тому пошукова команда повинна знати, що саме шукати.

7.6 Пакети Фарадея

З метою дотримання справедливості, електронні докази повинні бути захищені від втручання та факторів навколишнього середовища, які можуть завдати їм шкоди. Електронні докази дуже вразливі до електромагнітного випромінювання, а стандартні процедури роботи, зазвичай, передбачають застосування певного захисного заходу, що ґрунтується на принципі клітки Фарадея.

Майкл Фарадей – це науковець початку 19 століття, який став новатором у новітній науці про електричний струм. Він виявив, що якщо обклеїти кімнату металевою фольгою, а потім здійснити потужний електричний розряд (наприклад, за допомогою штучної блискавки), вимірювальна техніка всередині кімнати, захищеної фольгою, не зазнає впливу. Це відбулося в 1836 році, але на YouTube для перегляду доступні деякі сучасні демонстрації ефекту клітки Фарадея, що вражають уяву:

Клітка смерті Тесла (котушка Тесла генерує блискавку)

https://www.youtube.com/watch?v=Zi4kXgDBFhw

В Річарда Хаммонда в машині влучає блискавка

https://www.youtube.com/watch?v=ve6XGKZxYxA

Котушка Тесла і клітка Фарадея

https://www.youtube.com/watch?v=x7uCAvEhP1E

Як це застосовується до збереження електронних доказів?

По-перше, найкращою є практика забезпечення того, щоб електронні докази зберігалися протягом тривалого часу в приміщенні, яке захищене певною формою клітки Фарадея. По-друге, завжди рекомендується захищати електронні пристрої та докази під час їхнього переміщення з місця злочину до складу та/або експертно-криміналістичної лабораторії, використовуючи пакет Фарадея.

Пристрої, що містять електронні докази, повинні бути захищені від електромагнітних полів (можливо, за допомогою віддаленого доступу), використовуючи пакети Фарадея

Пакети Фарадея набувають різноманітних форм та розмірів: маленькі для телефонів, більші для комп'ютерів. Всі пакети мають однакову обшивку, яка перешкоджає впливу електромагнітного випромінювання на те, що міститься всередині них. Тут слід зробити застереження. Незважаючи на те, що пакети Фарадея дуже хороші і можуть запобігати, практично, будь-якому втручанню, як фактично і буває, переважно, певні радіочастоти та дуже потужні магнітні джерела в лабораторії можуть проникати в структуру пакету та впливати на те, що в ньому міститься.

Інша складність із пакетами Фарадея полягає в тому, що вони дорогі та не завжди доступні, особливо якщо вилучення не є результатом планового обшуку. Проте існують способи використання звичайних предметів для дому, які дають змогу досягти такої ж мети, якщо більш елегантні способи є недоступними.

Давайте спробуємо здійснити простий експеримент. Вам знадобиться два мобільних телефони (телефон А та телефон Б) та рулон звичайної домашньої алюмінієвої фольги.

1. Спочатку перевірте, чи працюють обидва телефони належним чином. Телефон А викликає Телефон Б (Не потрібно відповідати, просто переконайтеся, що телефон Б дзвонить, а потім зупиніть виклик);

2. Тепер обмотайте телефон Б алюмінієвою фольгою. Важливо, щоб телефон було повністю обмотано, а в фользі не було жодних проміжків чи дірок.

3. Тепер знову спробуйте скористатись телефоном А, щоб зателефонувати на телефон Б.

Якщо експеримент буде успішним, телефон А буде переведено на автовідповідач.

Цей експеримент демонструє швидкий і простий спосіб захисту електронних доказів (хоча він є не на 100% ефективним). Альтернативою, яку використовують деякі поліцейські служби, є використання металевої фарби – проте покриття повинно бути доволі щільним та закритим.

Одна цікава річ полягає у тому, що коли телефон Б буде знаходитися у фользі або в пакеті Фарадея, він перебуватиме поза діапазоном роботи базових станцій постачальника послуг, але телефон запрограмований на те, щоб намагатися під'єднатися через кожні кілька секунд або хвилин. Кожного разу, коли телефон Б намагається під'єднатися, він потребує живлення, відтак акумулятор телефону Б розрядиться дуже швидко. Це означає, що будь-які телефони, ізольовані в пакеті Фарадея, повинні мати пріоритет для вилучення та

вивчення, оскільки повне розрядження цих пристроїв означатиме, що експерту потрібно буде знати не лише PIN-код, але і PUK-код (Personal Unlocking Key).

Під час прийняття рішень щодо цифрових пристроїв та електромагнітних полів та всіх цих сучасних технологій легко забути про те, що традиційна криміналістична практика все ще відіграє важливу роль, навіть якщо мова йде про, виключно, електронні докази. Електронні докази, як ми раніше говорили, переважно є необов'язковими, і робота пристрою (носій, що має доказові дані) має бути остаточно пов'язана з підозрюваним. Відбитки пальців, ДНК, волоски та волокна можуть допомогти у встановленні цього зв'язку.

На місці злочину, також, важливо шукати речові докази, які можуть сприяти вивченню технології. Наприклад, багато людей зберігають паролі в зошиті або на аркуші паперу, прикріпленого до столу, у ящику чи навіть під клавіатурою. Також там можуть бути рахунки-фактури від постачальників послуг, які пропонують підписку на онлайн-сховище даних. Навіть такі речі, як книги на полицях, що стосуються обчислень, шифрування чи хакерства, можуть свідчити про те, що підозрюваний є освіченим у цій сфері, і доцільним у цьому випадку може бути більш досконале вивчення місця злочину (і жорсткого диска).

Не слід нехтувати традиційною судовою експертизою та збором речових доказів. Це доповнює та підкріплює електронні докази.

7.7 Шифрування

Шифрування було визначено як найбільша загроза для розслідування злочинів і призвело до появи явища, яке називається «піти в тінь». Цей термін використовується для опису складності доступу до зашифрованих електронних доказів навіть за рішенням суду.[26]

Іноді ми вживаємо слово «пароль», коли більш правильним було б слово «ключ шифрування», але щоб не створювати більшу плутанину ці терміни часто використовуються один замість іншого. Уявіть кімнату, захищену замкненими дверцятами, і ключ, який відкриває двері та дає вам доступ до всього, що знаходиться всередині. Іноді може існувати декілька подібних ключів, які можуть відкрити ці двері, або ж ви можете залізти туди через відкрите вікно. Опинившись усередині кімнати, ви маєте повний і необмежений доступ. Якщо пристрій, як і кімната, лише заблокований простим паролем (ключем), пароль надає вам можливість входу і отримання доступу до всіх даних.

Трохи інша ситуація виникає тоді, коли пристрій зашифровано. Існує лише один ключ шифрування, і все, що розташоване за дверима, настільки змінене, що навіть якщо ви можете будь-яким чином отримати доступ до вмісту пристрою, ви ніколи не зможете прочитати його. Шифрування проганяє всі нулі і одиниці через складне рівняння таким чином, що те, що виглядає як цілісна бібліотека структурованої інформації, стає сумішшю інформації, користуватися якою неможливо. Усі нулі та одиниці досі там, але вони розташовані в незрозумілому порядку, відновити який можна лише за допомогою правильного ключа шифрування.

[26] Comey JB (2015) Піти в тінь: шифрування, технології та баланс між громадськістю та конфіденційністю https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

Якщо слідчий має фізичний доступ до пристрою, «простий» пароль не обов'язково є перешкодою. Існує багато методів та прикладів програм, які дають змогу відкривати пристрій без пароля.

Проведіть швидкий тест зараз: якщо у вас є ноутбук із Windows або настільний комп'ютер, натисніть клавішу Shift на клавіатурі п'ять разів. Якщо з'являється спливаюче вікно, в якому виникає запитання, чи потрібно увімкнути клавіші, що залипають, то існує проста методика доступу до вашого комп'ютера за допомогою диска запуску Windows.

Іншим способом, який використовує спеціальне програмне забезпечення, є шина FireWire між вашим комп'ютером та заблокованим комп'ютером, яка разом з необхідним ПЗ надає вам доступ до даних.

Але якщо пристрій зашифровано, звичайне отримання доступу вам не допоможе.

Шифрування є основою для всієї діяльності в Інтернеті. Це дає змогу використовувати онлайн-банкінг або придбати речі в Інтернеті відносно безпечно. Обробка кредитної картки, потокове онлайн-відео чи використання електронної пошти залежать від шифрування. Все більше програм, таких як WhatsApp, здійснюють повне шифрування (тобто дані можуть бути прочитані лише відправником та особою, з якою ви спілкуєтеся). Програма Telegram настільки успішна в цьому, що в деяких країнах вона навіть була заборонена. Крім того, ми знаємо про анонімайзери, такі як Tor, що є доступними для вільного завантаження та використання.[27]

Шифрування зараз широко використовується, і всі версії Windows Professional (після Vista) мають функцію шифрування усього диска за назвою Bitlocker. Ще одним прикладом ПЗ в цьому контексті є VeraCrypt. Це безкоштовна програма, яка не тільки дає змогу шифрувати теку, але, також, створити спеціальний розділ на вашому жорсткому диску, який є як зашифрованим, так і повністю прихованим. Жодна особа, що здійснює пошук у теках комп'ютера, не може його бачити.

7.8 Зламування

Якщо ви не знайшли або не отримали пароль чи ключ шифрування, його треба або вгадати, або зламати. Технічні прийоми, які використовуються для зламування пароля або ключа доступу, є однаковими.

Ви можете запустити атаку «за словником», в якій слова в словнику або заздалегідь підготовленому переліку використовуються автоматично один за одним, або атаку методом «грубої сили», в якій кожна можлива комбінація великих та малих літер, цифр та спеціальних символів перевіряється на цільовому пристрої одна за іншою. Звісно, атака методом «грубої сили» може бути полегшеною, якщо відомо, що підозрюваний надає перевагу певним словам або темам чи використовує для свого пароля своєрідний формат; в такому випадку програмний інструмент може бути змінений для кращого зосередження на результаті.

[27] https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html

Проте ці типи атак можуть тривати кілька днів, і, якщо ключ шифрування буде досить складним, остаточного результату отримано не буде. На щастя, це буває зрідка. Більшість людей:

- використовують дуже прості паролі або ключі:
- використовують слова, назви або дати, які певним чином пов'язані з особою або з чимось популярним;
- не змінюють паролі, встановлені за замовчуванням;
- використовують паролі на різних пристроях (так що, коли буде знайдено один пароль, можна використати ті ж самі облікові дані, щоб отримати доступ до інших облікових записів).

Незважаючи на всю несприятливу рекламу, пароль «пароль», декілька клавіш, що стоять поруч та варіанти послідовності номерів 1234567 залишаються найбільш популярними за результатами опитувань.

Ось 10 найпопулярніших паролів 2018 року:[28]

1	123456
2	123456789
3	qwerty
4	password
5	111111
6	12345678
7	abc123
8	password1
9	1234567
10	12345

Якщо вам цікаво, чи було зламано будь-який з ваших облікових записів в мережі, спробуйте ввести свої дані тут

https://haveibeenpwned.com/

Якщо ваша електронна адреса є тут, краще змінити пароль просто зараз!

[28] https://www.mamamia.com.au/most-common-passwords/

Існує ймовірність того, що правильно зашифровані файли з сильним шифруванням неможливо зламати, і деякі пристрої, як ми зараз побачимо, містять додаткові заходи безпеки, спрямовані на недопущення того, щоб хтось вводив неправильний ключ занадто багато разів. Однак варто пам'ятати, що сила шифрування залежить від низки змінних:

- Міцності ключа;
- Обчислювальної потужності, що використовується для зламування ключа;
- Якості алгоритму шифрування, що використовується.

Насправді, за законом Мура, коди шифрування, які вважалися сильними лише декілька років тому, тепер зламані. Насправді, якщо квантові обчислення стануть комерційно рентабельними та доступними, наявні функції шифрування стануть застарілими в той самий день.

7.9 Основні закони про розкриття інформації[29]

Деякі країни вводять закони, які вимагають передавати його/її ключ шифрування, погрожуючи застосувати кримінальне покарання, але щодо цього були висловлені занепокоєння щодо права проти самообвинувачення. У деяких юрисдикціях, які ухвалили законодавство про розкриття інформації щодо ключів, законодавство обмежується в контексті захисту прав людини. Наприклад, Бельгія, Фінляндія або Нідерланди не дозволять застосовувати закон проти підозрюваного саме з цієї причини. З іншого боку, у Сполученому Королівстві закон було перевірено та затверджено в судах; і в разі відмови підозрюваної особи надати ключ шифрування, видається ордер для примусового надання, окрім того, таку особу буде покарано шляхом позбавлення волі строком до двох років, якщо йдеться про більшість злочинів, або до п'яти років, коли розслідування стосується національної безпеки або розбещення неповнолітніх.[30]

7.10 ФБР проти Apple

Проблеми, пов’язані з розкриттям інформації, що міститься у смартфоні, стали очевидними у справі «ФБР проти Apple».

2 грудня 2015 року сімейна пара Сайєд Різван Фарук і Ташфін Малік потрапили на корпоративну різдвяну вечірку в Inland Regional Center, що у Сан-Бернардіно, штат Каліфорнія, і відкрили вогонь. Вони вбили 14 осіб, ще 22 отримали тяжкі поранення. Терористів відслідковували протягом чотирьох годин, згодом вони загинули під час перестрілки з поліцією.

Перед атакою обидва терористи знищили власні мобільні телефони, але Фарук, який працював у Департаменті охорони здоров'я, також, мав робочий телефон Apple iPhone 5c, що належав Департаменту охорони здоров'я. Факти навколо того, що трапилося далі, нелегко розгадати, але, наскільки це можна констатувати, події відбувалися таким чином:

---

[29] Незважаючи на те, що Вікіпедію не можна вважати авторитетним джерелом для юридичних досліджень, вона має сторінку з основними законами про розкриття інформації. https://en.wikipedia.org/wiki/Key_disclosure_law

[30] Ось нещодавні випадки обговорюються тут: https://www.wired.co.uk/article/lucy-mchugh-murder-death-stephen-nicholson-facebook-password

- З абсолютно зрозумілих причин ФБР хотіло отримати доступ до iPhone Фарука, але телефон був зашифрований 4-значним PIN-кодом, а введення помилкового PIN-коду 10 разів поспіль цілком б стерло всю інформацію на пристрої (4-значний PIN-код може містити 10 000 різних комбінацій).

- На телефоні було увімкнене автоматичне резервне копіювання на обліковий запис Apple iCloud (який вимагав пароль, відомий Департаменту громадського здоров'я, який не був таким самим, як PIN-код Фарука).

- Резервні копії були незашифровані та їх можна було прочитати, але останнє оновлення копії було зроблене за шість тижнів[31] до атаки, і співробітники ФБР не могли бути впевненими в тому, що на iPhone містилася будь-яка корисна інформація (хоча той факт, що терористи вже знищили свої персональні телефони, давав змогу припускати, що її там не було).

- Тому, щоб отримати доступ до вмісту iPhone, співробітники ФБР просто могли зачекати до наступного автоматичного резервного копіювання.

Саме тут починаються розбіжності у поглядах на подальші події. Згідно з більшістю звітів, ФБР звернулися до Департаменту охорони здоров'я (власника телефону) і попросила змінити пароль iCloud, щоб запобігти доступу невідомого спільника терористів до облікового запису iCloud. На жаль, скидання пароля iCloud заблокувало функцію автоматичного оновлення.[32]

Відтак склалася така ситуація:

1. Існував iPhone із можливими доказами;
2. IPhone був зашифрований 4-значним PIN-кодом;
3. Введення помилкового PIN-коду 10 разів поспіль призведе до знищення пам'яті та будь-яких доказів;
4. Єдина людина, яка знала PIN-код, була мертва.

Тоді ФБР звернулося до суду з вимогою змусити Apple створити оновлення програмного забезпечення, яке б фактично порушувало безпеку iPhone і дозволило їм отримати інформацію. Компанія Apple відмовилася, пославшись на інтерес громадськості до захисту конфіденційності за допомогою шифрування. Компанія також стверджувала, що зробити це неможливо, але згодом змінила позицію, заявивши, що це можливо, але для цього необхідно залучити близько 10 фахівців, яким на написання такого програмного забезпечення потрібно близько місяця.

Аргумент конфіденційності зібрав шалену підтримку серед великої кількості суспільних вартових та IT-компаній. Створюючи такий прецедент, вони побоювалися, що поставлять під сумнів поняття особистого шифрування та знизять рівень інформаційної безпеки для кожної особи. Власне кажучи, вони мали рацію. Якби IT-компанія не змогла протистояти подібній вимозі в такій країні, як США, де права конфіденційності жорстко та юридично

[31] Різні звіти вказують різні періоди
[32] https://www.theverge.com/2016/2/22/11093798/apple-fbi-encryption-fight-icloud-san-bernardino

захищаються відповідно до Конституції, який тоді шанс на успішний опір у компаній, що існують у менш доброзичливих державах?

Справа розглядалася в судах до 28 березня 2016 року, коли ФБР раптово відкликала справу, заявивши, що їм все ж вдалося отримати доступ до iPhone. Ходять чутки, що цьому дуже посприяла ізраїльська компанія Cellebrite, яка є однією з провідних компаній у світі в сфері мобільних телефонів.

Досі невідомо, чи містилася на iPhone будь-яка важлива інформація. Було б, мабуть, цинічно стверджувати, що ФБР підлаштували обставини, щоб дозволити їм винести питання про шифрування до суду у випадку, коли факти справи викликали б у суспільства підтримку в такій вимозі. У будь-якому разі, доповідь про дії ФБР не знайшла загального схвалення.[33]

Незважаючи на те, що справа «ФБР проти Apple» не досягла етапу судового рішення, існує більш широка дискусія щодо етики та відповідності будь-якого законодавства, яке змушує виробників програмного забезпечення встановлювати інструменти обходу систем захисту у власній продукції. Для цього в законодавстві створено прецедент, згідно з яким американські телекомунікаційні компанії повинні створювати «точки доступу» для правоохоронного нагляду, але це працює виключно на національному рівні.[34] Будь-яке накладання подібних зобов'язань на програмні продукти матиме міжнародні наслідки.

7.11 Зламування правоохоронними органами

Є ще один можливий варіант, доступний правоохоронним органам для доступу до зашифрованих файлів: встановлення шкідливого програмного забезпечення на комп'ютер підозрюваного.

Справа Скарфо почалася у 2001 році. Нікодемо «Маленький Нікі» Скарфо був босом організованого злочинного угрупування, що діяло у Філадельфії. Під час розслідування його злочинної діяльності ФБР отримало судовий ордер на приховане встановлення на комп'ютері Скарфо такого програмного забезпечення, що називається Magic Lantern.[35] Це був складний кейлоггер. Іншими словами, він записував, які клавіші Скарфо натискав на клавіатурі комп'ютера (а також показував його історію веб-перегляду, логіни і паролі). Тоді ФБР вилучило комп'ютер і, після вивчення результатів роботи кейлоггеру Бюро мало доступ до зашифрованих файлів за допомогою облікових даних реєстрації Скарфо. Скарфо оскаржив використання цього шкідливого програмного забезпечення, стверджуючи, що був незаконний обшук відповідно до Четвертої поправки Конституції США, і звернувся до судді з проханням не враховувати всі наступні докази як «плоди отруєного дерева». Суддя відхилив його заяву, і Скарфо підписав угоду про визнання винуватості.

Суддя у справі, суддя Ніколас Політан, у своєму рішенні зазначив наступне:

---

[33] Спеціальне розслідування щодо точності заяв ФБР щодо можливостей Бюро використовувати iPhone, що вилучений під час розслідування теракту в Сан Бернардіно (березень 2018 року) https://oig.justice.gov/reports/2018/o1803.pdf

[34] Допомога у сфері зв'язку при прийнятті Закону про правопорушення https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[35] Заява офіцера ФБР, Спеціального агента Мерча, яка пояснює шкідливе програмне забезпечення, та як воно використовувалося, яку можна знайти за посиланням: www.epic.org/crypto/scarfo/murch_aff.pdf.

Нині кожного дня нам відкриваються нові пристосування, що вражають уяву, і які виготовлені за новітніми технологіями. Насправді, дивовижні можливості, що нам надає наука, часом просто неможливо уявити. Як наслідок, ми повинні бути дедалі пильними у тому, що стосується порушення конституційних прав з боку сучасних технологій. Однак, в той самий час, злочинці в наші дні, також, опановують технічні досягнення та використовують їх для просування своїх злочинних цілей. Кожного дня, сучасні комп'ютерні технології та підвищений доступ до Інтернету надають змогу ускладнити і розвинути кримінальну діяльність. Це, також, передбачає можливість знаходити нові способи вчинення старих злочинів, а також чинити нові злочини, які виходять за межі розуміння судів.[36]

Питання для перевірки знань:

1. Яку інформація можна втратити при вимкненому комп'ютері?

2. Чому небезпечно використовувати імена або слова зі словника у якості пароля або ключа?

3. Як робота Майкла Фарадея застосовується до цілісності електронних доказів?

Вивчення та огляд:

Як Ви вважаєте, що повинна містити Стандартна процедура роботи для відновлення електронних доказів?

[36] https://epic.org/crypto/scarfo/opinion.html

8 СПОСОБИ ВИЯВЛЕННЯ ПРИХОВАНИХ ФАЙЛІВ

Мета навчання:

Надання учасникам інформації щодо основних підходів до аналізу електронних доказів, а також тих методів, які використовують особи, що скоїли злочин, для приховування цих доказів.

8.1 Що відбувається у лабораторії?

Поліція провела обшуки та вилучила декілька електронних пристроїв. Ці пристрої були промарковані належним чином, описані в акті вилучення та поміщені в мішки Фарадея або були захищені іншим чином. Далі пристрої передаються до лабораторії криміналістичної експертизи для дослідження. Пам'ятайте про те, що ці пристрої є лише накопичувачами. Електронні докази містяться всередині них, і вилучати їх звідти повинен фахівець таким чином, щоб їхня цілісність була збережена.

Після того, як пристрої будуть отримані (і належним чином зареєстровані) лабораторією, з даних, що містяться на пристроях, робиться електронна копія. Накопичувач, на який завантажуються дані (звичайно, за допомогою «writeblocker»), повинен бути або новим, або бути повністю відформатованим. Це відбувається за допомогою процесу «заповнення нулями», під час якого кожен біт на накопичувачі отримує значення 0. Якщо не зробити цього, будь-яка інформація, що була на накопичувачі, потенційно може стати частиною копії.

Копія, що робиться для криміналістичної експертизи, відрізняється від звичайного резервування. Ця копія є точним дублікатом (що називається бітовий потік, побітове копіювання або клонування), яка відтворює кожен нуль і кожну одиницю з оригіналу. Але як фахівець може гарантувати, що копія справді є повним дублікатом оригіналу?

8.2 Хешування

Це можна зробити за допомогою процесу, який називається «хешування», під час якого створюється своєрідний цифровий відбиток, а саме довгий шістнадцятковий ($Base_{16}$) номер, який називають «хеш-значення».

Хешування є, з певного погляду, шифруванням, і коли для виконання відповідних розрахунків застосовується алгоритм хешу, отримане число або значення не може бути використане для зворотного визначення того, які значення були використані на початку. Розглянемо цю просту суму:

$$4 \times 5 \times 8 = 160$$

Якщо Ви знаєте результат (наприклад, 160) і який тип формули використовується, можна визначити, які значення могли бути використані під час початкового розрахунку, здійснивши зворотні обчислення. Існує обмежена кількість альтернативних значень, за використання яких можна досягти цього результату.

Наприклад:

4 x 4 x 10

або

4 x 2 x 20

або

2 x 16 x 5

тощо

Шляхом виключення можна встановити складові формули. Але з хешуванням все інакше – воно функціонує «в один бік», що означає, що навіть, якщо ви знаєте хеш-значення та використане рівняння, знайти або встановити вихідні значення просто неможливо. Ось чому процес хешування є дуже цінним контрольним механізмом.

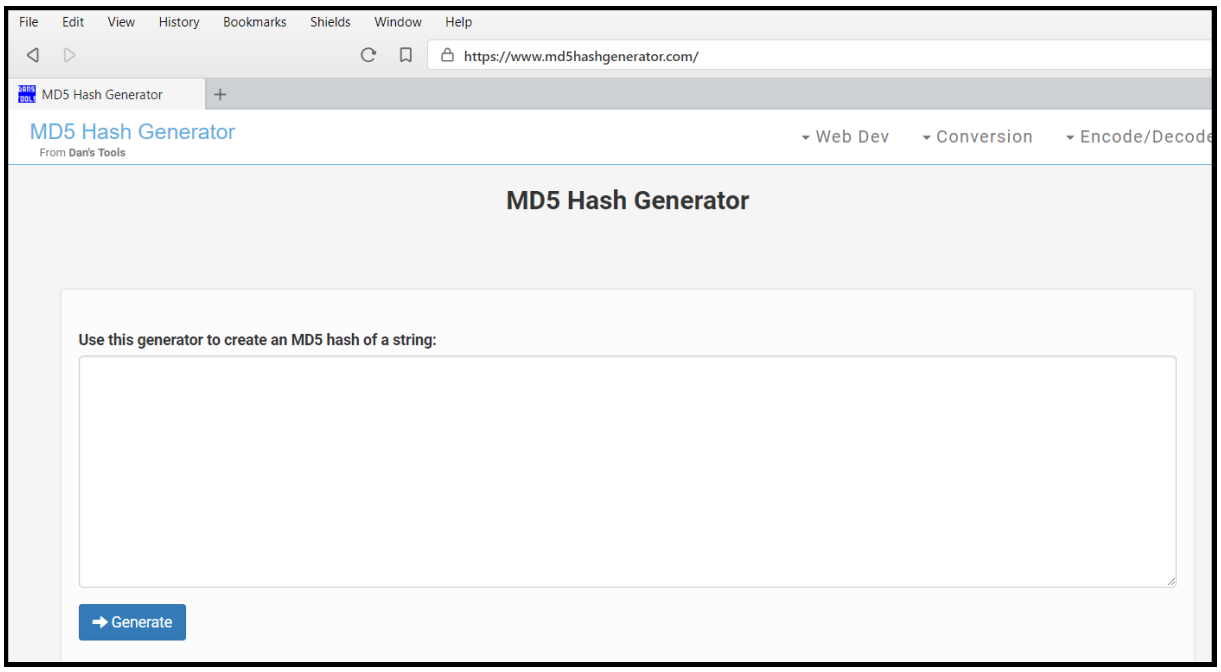
У лабораторії аналітик застосовує алгоритм хешування до оригінального диска та клону, а потім порівнює результати. Якщо значення хешування в обох випадках є однаковим, то для суду та судових експертиз контент цих двох файлів або дисків може вважатися точним дублікатом (існує малоймовірний шанс, що два хеш-значення можуть бути однаковими, попри неоднаковість контенту файлів, проте цей шанс є ще меншим, аніж для зразків ДНК).

Точність скопійованого жорсткого диска перевіряється шляхом застосування математичного рівняння, яке називається алгоритмом хешування до змісту оригіналу та дубліката. Коли хеш-значення змінюється, то копія є точним дублікатом.

Загалом використовуються два популярних алгоритми хешування: MD5 (скорочення від Message Digest 5) та SHA1 (скорочення від Secure Hash Algorithm 1). Ці системи були спочатку розроблені для шпигунської діяльності, але були зламані багато років тому і тепер вважаються небезпечними для шпигунів. Проте у разі цифрової криміналістики вони використовуються не для шифрування даних, а для перевірки однаковості відомого контенту. Поряд із тим, деякі фахівці надають перевагу використанню альтернативних алгоритмів хешування для запобігання виникнення будь-якої можливої критики з боку сторони захисту. Існує низка більш надійних алгоритмів хешування шифрування, включно із SHA-2, SHA 256 та SHA 512 (зауважте, що усі ці цифри є множниками числа 2), але вони дають набагато довші значення і потребують більше часу для виконання.[37]

Давайте проілюструємо процес хешування за допомогою MD5. В Інтернеті доступна велика кількість інструментів генерації хешу. В цьому випадку ми використаємо www.md5hashgenerator.com.

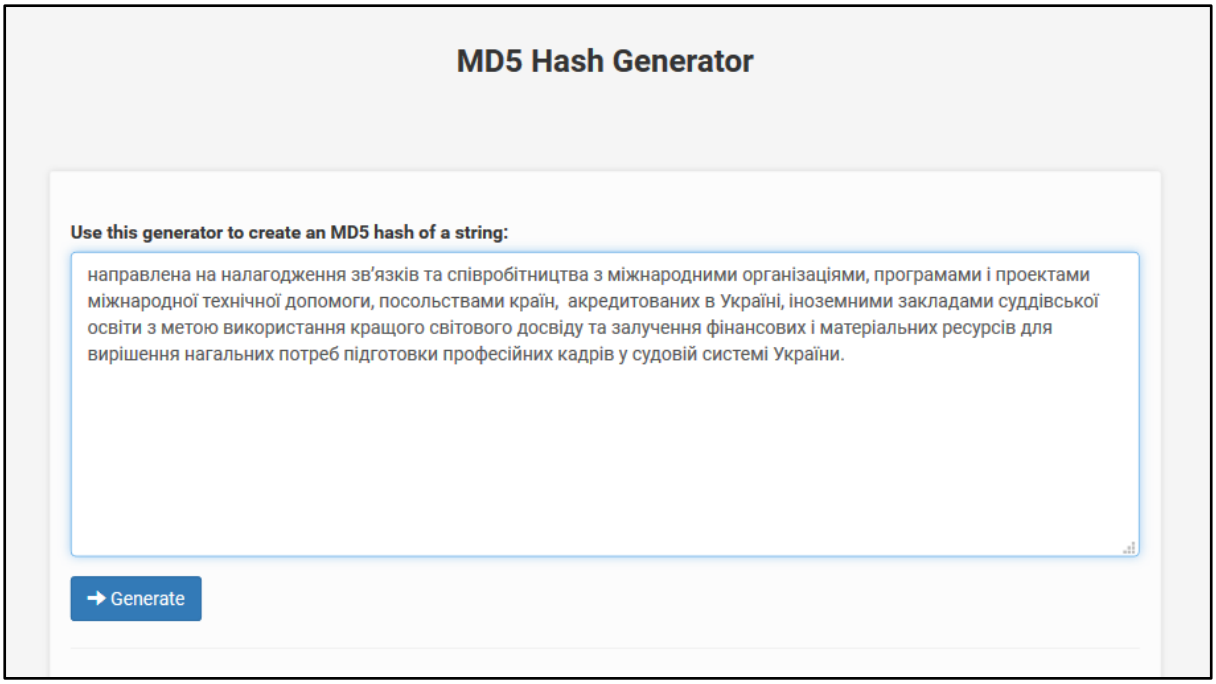
[37] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms



Якщо взяти розділ тексту, опублікованого на веб-сайті Національної школи суддів:

> направлена на налагодження зв'язків та співробітництва з міжнародними організаціями, програмами і проектами міжнародної технічної допомоги, посольствами країн, акредитованих в Україні, іноземними закладами суддівської освіти з метою використання кращого світового досвіду та залучення фінансових і матеріальних ресурсів для вирішення нагальних потреб підготовки професійних кадрів у судовій системі України.

Ми можемо ввести цей текст до онлайн-інструменту.



Після цього ми натискаємо кнопку «Генерувати (Generate)», щоб знайти MD5-хеш-значення

a17e03f6416902ac330a2ed4b6411a3b

Якщо ми виконаємо надзвичайно незначну зміну тексту, видаливши додатковий пробіл перед НШСУ посередині тексту

> направлена на налагодження зв'язків та співробітництва з міжнародними організаціями, програмами і проектами міжнародної технічної допомоги, посольствами країн, акредитованих в Україні, іноземними закладами суддівської освіти з метою використання кращого світового досвіду та залучення фінансових і матеріальних ресурсів для вирішення нагальних потреб підготовки професійних кадрів у судовій системі України.

І повторимо процедуру, алгоритм створить зовсім інше хеш-значення.

Нове хеш-значення: 8314a628e737ad6913bf197c14840970

Потрібно змінити лише один нуль або одиницю в одному біті, щоб створити абсолютно інакше значення хеш-значення.

Саме так судовий експерт може гарантувати точність копії. Після цього дослідник буде продовжувати проводити всі дослідження, використовуючи копію, зберігаючи при цьому оригінал даних у захисному кейсі у випадку будь-яких суперечностей щодо його висновків.

Потрібно змінити лише один 0 або 1 у файлі, щоб хеш-значення було зовсім іншим.

8.3 Зберігання даних

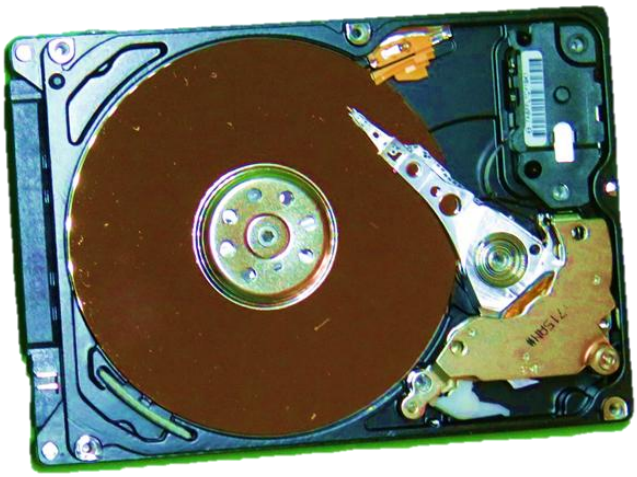
Не так давно дані зберігалися на магнітній стрічці або у вигляді паперових стрічок або карток з отворами в них. Незважаючи на дослідження, спрямоване на спроби створити носії для зберігання інформації про усі матеріальні об'єкти – від ДНК до алмазів та рідин, існує три основні способи збереження цифрових даних:

- Магнітні носії – як жорсткі диски
- Оптичні носії – CD-диски та DVD-диски
- Крихітні світчі або транзистори, розташовані на мікрочіпах – на твердотільних накопичувачах та флеш-накопичувачах

Ці форми зберігання ґрунтуються на принципі, що полягає в тому, що об'єкт зберігання може перемикатися між станами вмикання та вимикання.

Жорсткі диски (HDDs)

Жорсткий диск – це загальновизнана технологія, яка продовжує бути популярною, незважаючи на деякі недоліки розробки.



Його робота дуже схожа на старомодний грамофон. У звичайному домашньому комп'ютері диск із магнітним покриттям обертається на швидкості 7200 обертів на хвилину (диски у деяких комерційних серверах обертаються зі швидкістю, що понад вдвічі перевищує швидкість звичайних дисків). У режимі читання головка рухається його поверхнею та зчитує інформацію про те, чи частинка увімкнена (тобто має значення 1) або

вимкнена (значення 0). Якщо комп'ютер перебуває в режимі запису, головка буде намагнічувати або розмагнічувати частинку за потреби.

Оскільки це механічний пристрій, рухомі деталі можуть бути спрацьовані або пошкоджені внаслідок недбалого зберігання. Швидкість, з якою можна записати або зчитати дані, також, обмежується ефективністю механічних частин. Оскільки дані зберігаються магнітно, негативний вплив на них може бути також спричинений магнітним полем або екстремальними температурами.

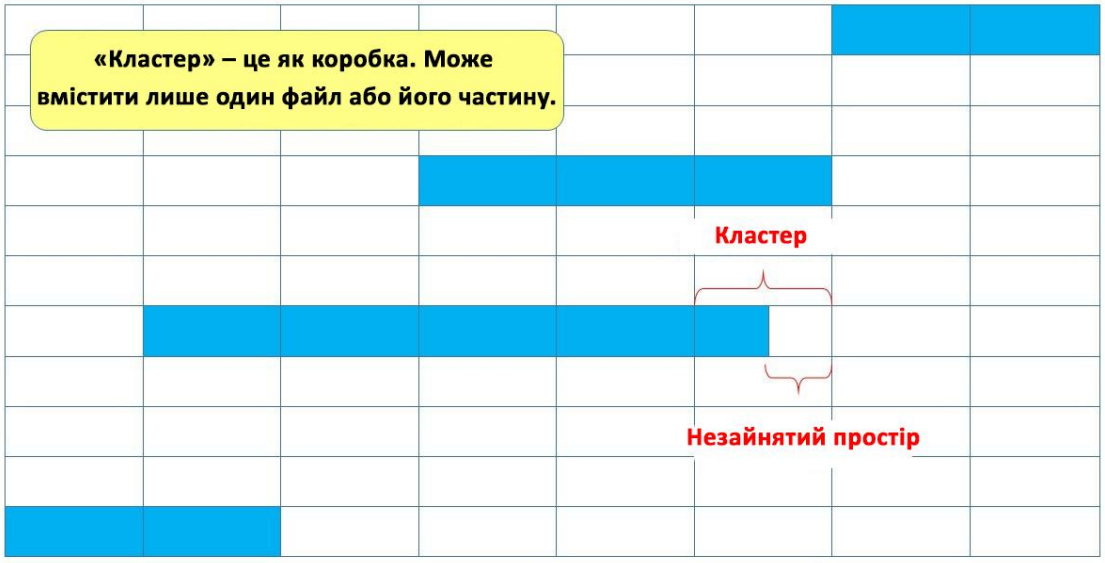
Зберігання даних на жорстких дисках

Оскільки вони залишаються найпопулярнішими варіантами, що використовуються найчастіше, давайте більш детально розглянемо, як дані зберігаються на пристрої з ОС Windows та жорстким диском.

Поверхня диска розбита на концентричні доріжки. Діаметр жорсткого диску комп'ютера становить 3 ½ дюйма, а кожен диск може мати тисячу доріжок (треків). Кожен трек підрозділяється на маленькі невидимі коробочки за назвою «кластери». Розмір цих кластерів залежить від типу файлової системи, що використовується, але середній розмір становить 512 байт (хоча вони можуть бути набагато, набагато більшими).

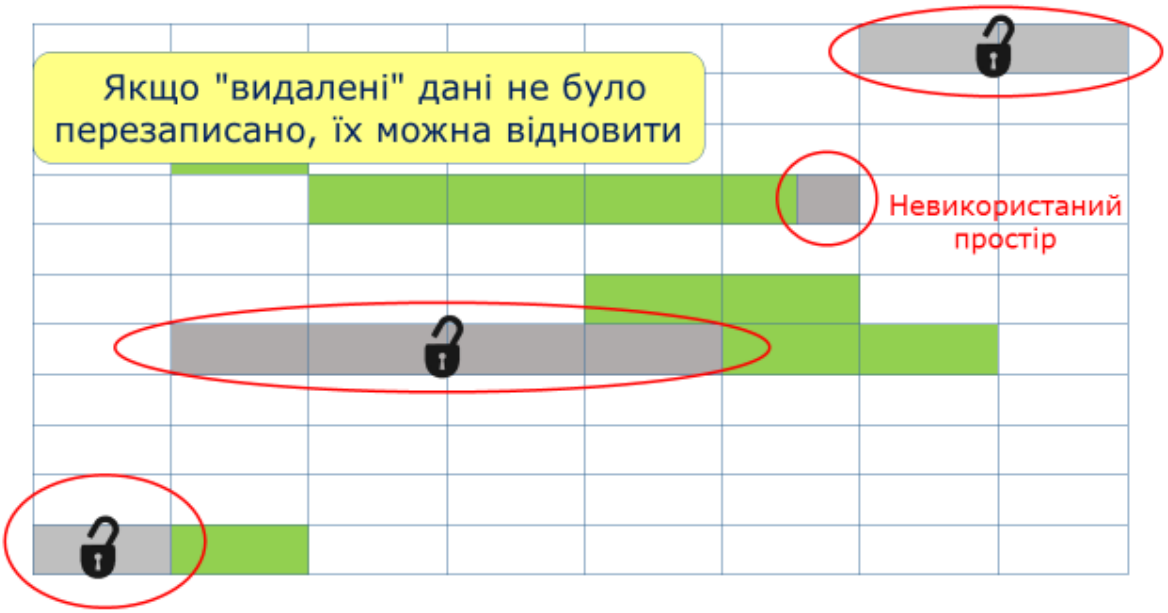
Коли файл зберігається на диску, він зберігається в будь-яких доступних і зручних для цього кластерах. Кластери або ящики, в яких зберігається файл, не повинні обов'язково бути розміщені поряд та можуть бути «фрагментовані» в різних місцях. На диску міститься невеличке програмне забезпечення, що називається Основна Таблиця Файлів, яке є своєрідним алфавітним покажчиком або картотекою та здійснює записи про те, що там розміщено, і блокує ці кластери від подальшого використання.

Важливо також знати, що кластер – це найменша одиниця на диску, яка може містити дані, і що кожен кластер може лише зберігати дані з одного файлу або частини цього файлу.



Кластер - це найменша одиниця пам'яті, яку можна призначити файлу. Однак він може містити лише один файл або частину файлу одночасно.

Уявіть це таким чином – ви пишете роман і встигаєте повністю заповнити 4 коробки набраними сторінками рукопису, але у вас залишилося достатньо сторінок для заповнення половини п'ятої коробки. П'ята коробка тепер не може бути використана для чогось іншого (якщо, звісно, ви не вирішите продовжити свій роман, у цьому випадку ви можете відкрити п'яту коробку і заповнити її). Потім усі коробки позначаються іменем файлу («Мій роман»), скріплюються печаткою та зберігаються в шафі. Простір, що залишився невикористаним у кластері (порожній простір у п'ятій коробці) відомий як «незайнятий простір».



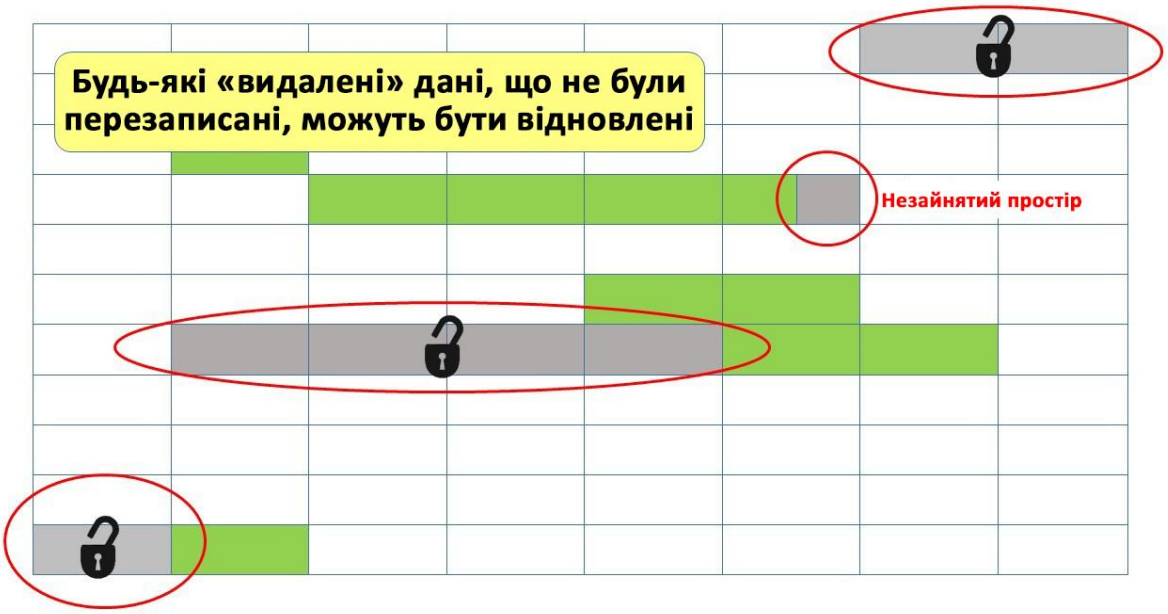
У шафі, можливо, вже є інші предмети на полицях, тому вам доведеться поставити ящики, де ви можете, у порожніх місцях.

Усі коробки з цим файлом («Мій роман») захищені. Вони захищені доти, допоки ви не натиснете на кнопку видалення. І все ж, навіть якщо ви натиснули на кнопку «видалити», з даними на диску нічого не трапилося. Відбувається лише ось що: запис у Основній Таблиці Файлів змінюється, а кластери (коробки) позначаються як вільний простір для повторного використання. Файл даних не змінюється. Саме тому, навіть коли документ видалено, файл відновити все ще можливо. Єдиний спосіб переконатися, що файл дійсно видалено – це скористатися програмою, яка називається «шредер файлів». У світі матеріальних речей шредер розрізає паперовий документ на дрібні частини таким чином, що їх не можна знову скласти разом. На комп'ютері шредер проходить через відповідні кластери, скидаючи біти на нуль (для певності цю процедуру на диску необхідно виконати декілька разів).

Якщо ви не використовуєте шредер файлів, файл залишатиметься доти, допоки ви не збережете новий файл, і комп'ютер буде змушений повторно використовувати ті ж самі

кластери. Коли це трапляється, комп'ютер «перезаписує» кластер з новими даними.[38] Але принцип незайнятого простору все ще застосовується. Якщо кластер раніше був заповнений даними, а новий файл лише частково перезаписує його, то можливість зчитати всі залишки попереднього файлу в невикористаній частині кластера все одно залишиться. Це небагато – але це краще, ніж нічого.

Будь-які дані, що зберігаються на комп'ютері, залишаються там, доки їх не буде перезаписано новим файлом або стерто з програмою «шредер файлів».



Оптичні накопичувачі:

Як вже було зазначено, оптичні накопичувачі також використовують диск, що обертається, але покриття на диску виконується з алюмінію або золота, а дані зчитуються або записуються лазером. У режимі запису лазер використовує тепло, щоб випалити дрібні виступи на поверхні диска, які називаються «лунки». У режимі читання лазер реєструє зміни на поверхні диска. Якщо диск рівний, лазер читає одиницю, але там, де він бачить лунку, диск не відбиває лазер, який реєструє лунку як нуль.

Твердотільні накопичувачі (SSDs):

Мікросвітчі або транзистори використовуються для зберігання інформації як на флеш-пам'яті, так і на USB-картах і флеш-картах, але у випадку їхнього використання у твердотільних накопичувачах (SSDs) вони забезпечують ефективну альтернативу жорстким дискам як основну можливість зберігання даних для будь-якого комп'ютера.

Вони надійні, менш чутливі до впливу рухів, ударів та не реагують на електромагнітні поля. Вони також набагато ефективніші – можуть зберігати більше даних у певному просторі та не генерують тепло, що створюється рухами механічних частин жорсткого диску. Це

[38] Існує припущення, що навіть після цього використання електронного мікроскопа може дати достатню кількість старих бітів для відтворення даних.

означає, що конструкція пристрою не потребує створення додаткових елементів охолодження. Обробка даних, також, відбувається набагато швидше. Однак, SSDs значно дорожчі, ніж жорсткі диски, крім того існує, принаймні, теоретичне обмеження кількості разів увімкнення або вимкнення мікросвітчів, перш ніж вони починають відмовляти.

Звичним є явище, коли пристрої мають жорсткий диск та твердотільний накопичувач, або коли в комп'ютері міститься одразу декілька накопичувачів, що працюють разом.

8.4 Різні файлові системи

Ми розглядали, як дані зберігаються за допомогою операційної системи Windows. Фактичний механізм залежить від конкретної «файлової системи», що використовується. Кожен тип операційної системи має інший спосіб зберігання даних і часто використовує декілька файлових систем. Кожна файлова система має свої особливі схеми і вимагає спеціальних знань від експерта.

У Microsoft Windows існує чотири файлові системи, про які варто знати, і які, ймовірно, будуть зазначені у висновку судового експерта. Кожна з них має змогу оперувати різним максимальним розміром файлу.

Файлова система Windows	Максимальний обсяг зберігання
FAT (File Allocation Table) 16	2GB
FAT 32	32GB
NTFS (New Technology File System)	16 EB[39]
exFAT (Extended FAT)	16 EB[40]

Оскільки вимоги до обчислень зросли, зросла і потреба створення більш потужних файлових систем. FAT 16 зараз є вже непрактичною, враховуючи розмір сучасних програм та файлів. Навіть більш сучасна FAT 32 з максимальним обсягом у 32 Гб вважається недостатньою. Зараз більшість систем Windows використовують NTFS, яка має неймовірний в теорії максимальний розмір файлу (при правильному налаштуванні) – 16 ексабайтів[41]. На жаль, для нормальної роботи NTFS потребує багато комп'ютерної пам'яті, тобто займає місце, яке можна було б використовувати для зберігання файлів. У зв'язку із цим було розроблено менш ресурсномістку файлову систему exFAT. Вона потребує менше ресурсів (і займає менше місця) та, переважно, використовується у USB-картах пам'яті/флеш-накопичувачах та SD-картах.

[39] http://www.ntfs.com/ntfs_vs_fat.htm.
[40] http://www.ntfs.com/exfat-comparison.htm
[41] 1 Exabyte = 1,000,000,000,000,000,000 bytes

Операційні системи Apple використовують файлову систему, що називається HFS+, а операційна система з відкритим кодом Linux використовує ext2, ext3 і ext4. З великої четвірки операційних систем залишилася лише ОС Android. Не без певної частки гумору розробники Android (що належить компанії Google) назвали свою систему «Ще одна файлова система Flash» (Yet Another Flash File System, YAFFS).

8.5 Приховування файлів

Існує кілька десятків способів приховування файлів на комп'ютері. Наприклад, ми вже обговорили, як можна створювати невидимі розділи за допомогою програмного забезпечення для шифрування, такого як VeraCrypt[42].

Неправильно позначені файли

Можливо, найпростіший спосіб приховати файл – це інакше позначити його, і навряд чи він стане предметом уваги слідчого. Всі файли мають призначені їм властивості, які можна видалити або змінити, щоб спотворити результати пошуку.

Відкрийте файл Word, потім перейдіть до меню Файл (у верхньому лівому куті). Коли відкриється вікно Інформація, у нижньому правому кутку вікна з'явиться посилання: «Показати всі властивості». Тут Ви побачите, чи додані будь-які ключові слова, ім'я власника файлу тощо. Якщо Ви не хочете, щоб допитливий слідчий шукав усі файли, що позначені Вашим ім'ям, Ви можете змінити цю інформацію.

Для додаткової безпеки Ви, також, можете змінити розширення файлів. Розширення файлу – це три або чотири літери, які з'являються після точки. Вони повідомляють комп'ютеру, яку програму слід використовувати для відкриття документа. Якщо розширення файлу є невірним, комп'ютер не зможе відкрити файл.

Ось деякі загальні розширення файлів:

.docx	.pptx	.xlsx	.txt
.mp3	.wav	.tiff	.jpg
.exe	.zip		

З них .exe є виконуваним файлом, іншими словами, він є програмою, а не документом, а .zip є текою, в який стиснуто декілька файлів (файлів з усім надлишковим повітрям вичавленим з них, щоб вони заповнили менший простір).

Якщо ви спробуєте змінити розширення файлу, комп'ютер попередить вас, що файл може стати непридатним для використання, але це саме те, чого ви хочете. Як бонус, відповідна піктограма з файлом, також, зміниться.

[42] Декілька років тому дуже популярним було програмне забезпечення для вільного шифрування за назвою TrueCrypt, але проект було припинено, а програмне забезпечення більше не підтримується. Його місце зайняла програма VeraCrypt, але TrueCrypt все ще використовується (попри ризики безпеки).

Що це означає на практиці? Ну, припустимо, що корумпований користувач на своєму комп'ютері має таблицю Excel. Якщо він/вона хоче убезпечити інформацію від чужих очей, то може змінювати як назву файлу, так і розширення файлу (а також будь-які властивості, що відстежуються) і зберігати файл у теці з фотографіями з торішньої відпустки.

Замість:

Briberyaccounts.xlsx

Він/вона може зберегти файл як:

Seaside.jpg

Цей метод приховування не є захистом від помилок, і ретельний експерт може помітити розбіжність між файлом та його підписом у пам'яті (виконуючи процедуру, яка називається Аналіз розширення файлу), але тільки якщо він/вона шукає його. Криміналістика у сфері цифрових технологій – це робота, що вимагає ретельності, надзвичайних обсягів роботи та концентрації, і з огляду на величезний обсяг тек і файлів на пристрої помилковий файл також може бути пропущений.

8.6 Стеганографія

Слово «стеганографія» походить від *грецького steganos*, що означає «прихований» та *латинського graphia*, що означає «писати». У давні часи пергамент був дорогим, тому було розроблено спосіб переробки письмових повідомлень. Шматок бджолиного воску розмазувався по глиняній дощечці, а повідомлення наносилося на воску за допомогою стилусу. Далі раб або слуга доправляв дощечку до місця призначення. Коли одержувач повідомлення хотів відповісти, він або раби розтоплювали віск і розгладжували поверхню, таким чином видаляючи перше повідомлення. Після цього повідомлення наносилося на розгладжений віск.

Але що, якщо було потрібно надіслати секретне повідомлення? Спочатку на мокру глиняну дощечку наносилося перше повідомлення, далі воно покривалося бджолиним воском, на який вже наносилося якесь звичайне повідомлення. Таким чином, якщо дощечку хтось перехопив би, існував високий шанс того, що справжнє повідомлення залишиться непоміченим. Повідомлення було покрито або сховано під воском.

За умов комп'ютерної ери стеганографія може бути виконана з будь-яким типом файлу: аудіо, текстом або зображенням. Наприклад, розглянемо одну систему стеганографії з зображеннями.

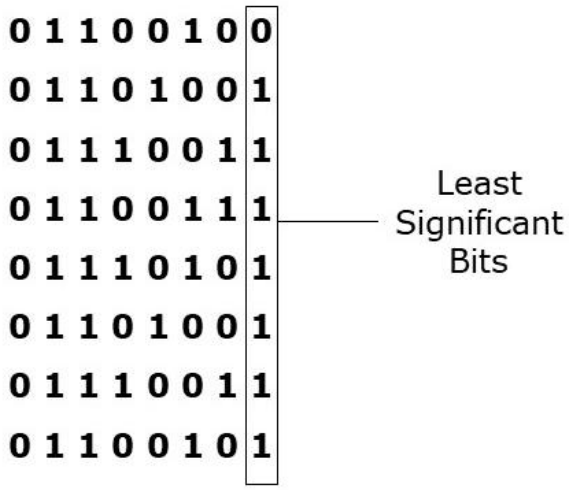
Кожен байт має один конкретний біт, який можна змінити, не змінюючи цілісність байту чи впливаючи на його загальний зміст. Цей біт називається найменш значним бітом (Least Significant Bit, LSB), і за порядком цей біт є восьмим в байті (тобто розміщений найдалі від правого).

Літерою S у бінарному коді є:

01010011

Біт, що стоїть справа, є найменш значущим бітом (Least Significant Bit, LSB)

Тепер припустимо, що ми хочемо сховати цю літеру S (яку ми будемо називати корисним навантаженням) серед бітів файлу зображення .jpg (який ми називатимемо файлом-носієм). Оскільки буква S складається з 8 біт, нам потрібно буде подивитися на 8 LSB (8 байт) із бінарного коду зображення.



У цьому методі кожен біт корисного навантаження почергово порівнюється із LSB в коді носія. Почнемо з порівняння першого біта з корисного навантаження з LSB першого байта фотографії (носія):

Корисне навантаження 01010011

Носій 01100100

Допоки вони збігаються, робити нічого не потрібно. Аналогічно, перевірка другого біта у букві S у LSB другого байта також не дає змін.

Корисне навантаження 01010011

Носій 01101001

Але, якщо порівняти третій біт з третім LSB, виникає розбіжність:

Корисне навантаження 01010011

Носій 01110011

Це означає, що LSB носія необхідно змінити для того, щоб тексти збігалися.

01110010

Це побітове порівняння між нашим повідомленням (корисним навантаженням) та LSB носія продовжується до того моменту, допоки вихідний код носія:

01100100 01101001 01110011 01100111 01110101 01101001 01110011 01100101

не буде змінено до:

01100100 01101001 01110010 **01100111 0111010**0 **0110100**0 **01110011 01100101**

Для цього треба було змінити лише три з восьми бітів (тобто 37,5%). Якщо зараз перевірити всі LSB, Ви побачите, що вони збігаються зі значенням корисного навантаження:

0 1 0 1 0 0 1 1

Це лише один з декількох стеганографічних підходів[43]; безумовно, реальне стеганографічне програмне забезпечення є небагато складнішим. Вони змішують LSB непередбачуваними способами. Але з погляду людського сприйняття, це ні на що не впливає, оскільки фотографія буде виглядати так само.

LSB - це один біт в байті, який, якщо змінити, буде мати найменший вплив на значення байту в цілому.

Виявлення стеганографії може бути дуже складним у випадку, якщо відсутня інформація про її наявність та використаний тип стеганографічного алгоритму. Якщо експерт має дві версії одного і того ж файлу, то можна порівняти розмір і структуру файлів. Є також програмні засоби, які дають змогу порівнювати характеристики файлів та виконувати пошук структурних аномалій, які можуть вказувати на наявність стеганографічно змінених файлів.

8.7 Журнали

Ми вже відзначали, як все, що здійснюється комп'ютером чи за допомогою комп'ютера, фіксується або записується певним чином. Журнали спочатку створювалися для того, щоб допомогти відстежувати будь-які помилки чи проблеми у разі некоректного функціонування програмного забезпечення. Іншими словами, вони були і є адміністративним інструментом. Але з огляду на той факт, що журнали, також, фіксують, як використовувався пристрій, а також те, що робив користувач, вони можуть надати дуже корисні докази.

Журнали можуть містити:

- Пошукові терміни
- Відвідані веб-сайти
- Перелік програм, що відкривалися, та користувач, що здійснював таку дію
- Створені та видалені документи
- Сервіси, що використовувалися
- Надіслані та отримані електронні листи
- Паролі та інші реєстраційні дані для входу
- Будь-які вибрані налаштування

[43] https://securelist.com/steganography-in-contemporary-cyberattacks/79276/

Більшість програм створюють журнали, які записують, що відбувається на комп'ютері.

8.8 Історія перегляду веб-сторінок

Нині існує безліч браузерів для серфінгу в мережі. За замовчуванням на комп'ютерах Windows використовувався Internet Explorer (IE), але тепер його замінено на Microsoft Edge. Відтак раніше упродовж багатьох років IE був найпопулярнішим браузером, але декілька років тому він втратив цей статус.

Це останні статистичні дані про найпопулярніший браузер за статистикою Вікіпедії[44]

Браузер	StatCounter Червень 2018 року	NetMarketShare травень 2018 року	Wikimedia Травень 2018 року
Chrome	58,9%	60,60%	47,77%
Safari	13,70%	17,27%	22,16%
UC	7,46%	1,69%	0,32%
Firefox	5,17%	5,89%	6,21%
Opera	3,50%	2,07%	1,16%
Internet Explorer	3,12%	5,85%	7,30%
Samsung Internet	2,67%	н/д	0,74%
Edge	1,89%	2,06%	1,93%
AOSP	1,56%	1,10%	1,02%
Інші	2,01%	3,47%	11,39%

Можна, також, переглядати Інтернет «інкогніто» або «конфіденційно», що означає, що Ваш комп'ютер не зберігатиме Вашу історію веб-перегляду, але навіть технічно освічені користувачі забувають про це.

Наприклад, інженер-програміст Мохаммед Амер Алі повинен був знати про це більше. Він увійшов у DarkNet, використовуючи нікнейм «Wierdos 0000», і намагався купити хімічну зброю, а саме отруту, що називається рицин, і яка виготовляється з рицинового насіння. Алі пояснили, що отрута буде доправлена до нього додому в іграшковій машинці.

[44] https://en.wikipedia.org/wiki/Usage_share_of_web_browsers Вікіпедія не обов'язково є надійним або авторитетним джерелом, і будь-яка важлива інформація, отримана звідти, завжди повинна бути перевірена.

На щастя, насправді він намагався купити зброю у агента ФБР під прикриттям, який патрулював «темну мережу»[45]. Завдяки співпраці між ФБР та владою Великобританії, його згодом заарештували та засудили, і зараз він відбуває 8-річний строк ув'язнення.

Під час обшуку його комп'ютера в його історії пошуку в Google було виявлено запит про відносну потужність абріну (іншої отрути) та рицину, а також запити про виготовлення ціаніду та рицину за домашніх умов. На його мобільному телефоні було виявлено запит в Yahoo: «Яка отрута вбиває швидко, є надійною, яку легко знайти/виготовити, легко приховати і важко виявляти під час патологоанатомічного огляду».

Можливо, так само важливо знати, що трапляється, коли експерт-криміналіст припускається помилки.

У справі Кейсі Ентоні мати-одиначку було виправдано під час судового засідання у справі про вбивство її маленької дочки на ім'я Кейлі. Тіло дворічної Кейлі було знайдено через 6 місяців після її зникнення; воно було дуже сильно розкладене, закутане в ковдру та містилося всередині сміттєвого мішка. Його знайшли в полі неподалік від дому, де проживає її сім'я. Обвинувачення стверджувало, що Кейлі була введена до несвідомого стану хлороформом, а потім була задушена липкою стрічкою поверх носа і рота. Під час судового розгляду було надано докази того, що сімейний комп'ютер (на момент вчинення злочину Ентоні жила разом з її батьками) було використано для пошуку слова «хлороформ» 84 рази. Прокуратура подала цей факт як доказ про наміри. Проте використане програмне забезпечення було неточним, і коли перевірка була здійснена розробником програмного забезпечення, з'ясувалося, що пошуковий термін «хлороформ» фактично здійснювався лише одного разу. Судовий процес все ще тривав, і цей експерт звернувся до прокуратури з новою інформацією. Проте виявилося, що це звернення було проігнороване стороною обвинувачення.[46] Тоді матір надала свідчення, що вона помилково ввела слово «хлороформ», хоча насправді хотіла здійснити пошук за словом «хлорофіл» (таким чином, піддаючи сумніву версію подій судового переслідування).

Історія перегляду веб-сторінок на комп'ютері сім'ї Ентоні була частково видалена, але кримінальні експерти стверджують про можливість визначення низки інших пошукових термінів, здійснених протягом 15-хвилинного періоду часу, включно із:

- Хлороформ
- Вдихання
- Алкоголь
- Смерть
- Самозахист
- Травми голови

І додаткові пошуки в інший час:

[45] Задіяння агентів під прикриттям для упіймання злочинців в «темній мережі» - це ще одна тема, яку можна обговорювати увесь день.
[46] https://www.johntfloyd.com/prosecutorial-misconduct-in-casey-anthony-case/

- Перелом шиї
- Як зробити хлороформ
- Виготовлення зброї
- Внутрішня кровотеча
- Смерть

Але у зв'язку із частковим видаленням було неможливо сказати, хто був автором цих пошуків.[47]

Розглянувши сукупність доказів, через 10 годин і 40 хвилин присяжні визнали Ентоні невинуватою у вбивстві першого ступеня. Сторона обвинувачення не змогла довести свою правоту, але після судового розгляду з'явилася додаткова інформація про історію перегляду, коли адвокат Ентоні опублікував книгу.[48] Він стверджував, що надав комп'ютерні дані власному експерту-криміналісту в цифровій сфері, який виявив, що в останній день, коли Кейлі бачили живою, у Google було здійснено пошук «fool-proof suffication», що перекладається як «гарантоване придушення» (за умови того, що у слові «suffication» було зроблено помилку, оскільки правильним варіантом є «suffocation»). Цей пошук було здійснено за допомогою браузера Firefox, але, як припускалося, правоохоронні органи під час вивчення жорсткого диска вивчали історію веб-перегляду лише в Internet Explorer. Зазначалося, що Ентоні надавала перевагу браузеру Firefox у використанні. Через хвилину після пошуку «fool-proof suffication» користувач комп'ютеру зайшов до соціальної медіа-платформи MySpace (яку Ентоні часто відвідувала).[49]

Ентоні було визнано невинуватою у вбивстві[50], а цифрові докази були лише однією частиною справи обвинувачення[51], але, власне, справа ілюструє найкращу практику в порівнянні з невдалими прийнятими рішеннями у справі:

- Експерт-криміналіст повинен знати, що він робить;
- Висновки мають бути підтверджені кількома програмними засобами;
- Програмні засоби повинні бути перевірені перед використанням;
- Ви не можете вивчати лише одну область або аспект даних на пристрої. Там можуть бути докази, що приховані в іншому місці;
- Існує потреба пов'язувати підозрюваного з використанням пристрою (що було б можливим у цій справі з доказом відвідування MySpace і, можливо, помилкою у пошуку із задушенням та тим фактом, що підозрювана у питанні використання браузеру надавала перевагу Firefox).

---

47 https://www.christianpost.com/news/casey-anthony-trial-computer-search-terms-include-internal-bleeding-death-chloroform-50988/

48 Baez J (2012) *Presumed Guilty, Casey Anthony: The Inside Story*

49 https://www.dailydot.com/news/casey-anthony-browser-history-suffocation/

50 Попри це вона була обвинувачена у вчиненні чотирьох проступків (включно із наданням правоохоронним органам неправдивих свідчень) і засуджено до чотирьох років позбавлення волі.

51 Враховуючи експертні свідчення про факт розкладання тіла у автомобілі Ентоні та того факту, що про зникнення Кейлі ніхто не повідомляв протягом 4 тижнів.

Ґрунтуючись на вивченні деяких питань, пов'язаних з справою Ентоні, та її історії веб-перегляду, нижче наведено деякі відомості про те, як Ваш комп'ютер записує Вашу поведінку в Інтернеті.

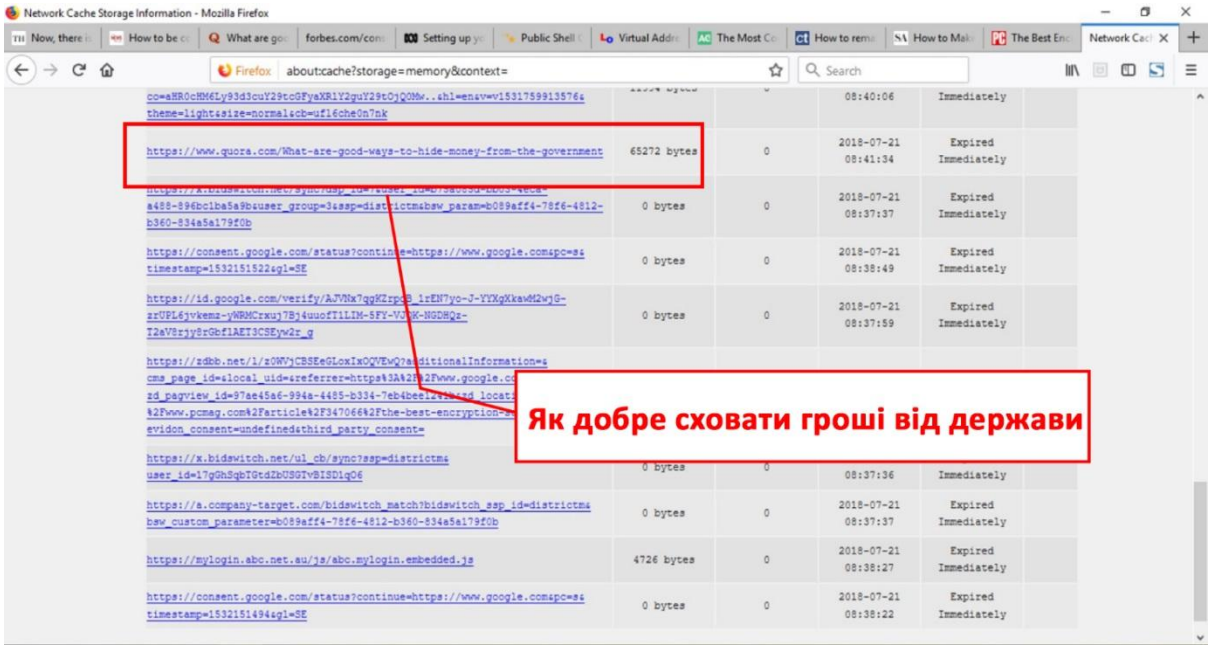
Ми проілюструємо це, скориставшись Firefox і вставивши about:cache до адресного рядку.

Коли Ви вводите about:cache, Ваш браузер Firefox негайно відкриє сторінку, що називається «Служба зберігання мережевого кешу (Network Cache Storage Service)». Натискання на посилання «Список кеш-записів» покаже довгий список посилань на інтернет-адреси. Цей список нелегко прочитати через функції перегляду веб-сторінок. Веб-сторінка складається з великої кількості різних елементів, які не завантажуються усі відразу, а послідовно за раз. Після завантаження всіх елементів браузер об'єднує їх. Те, що ми бачимо на сторінці «Кеш-записів», є окремими елементами веб-сторінки.

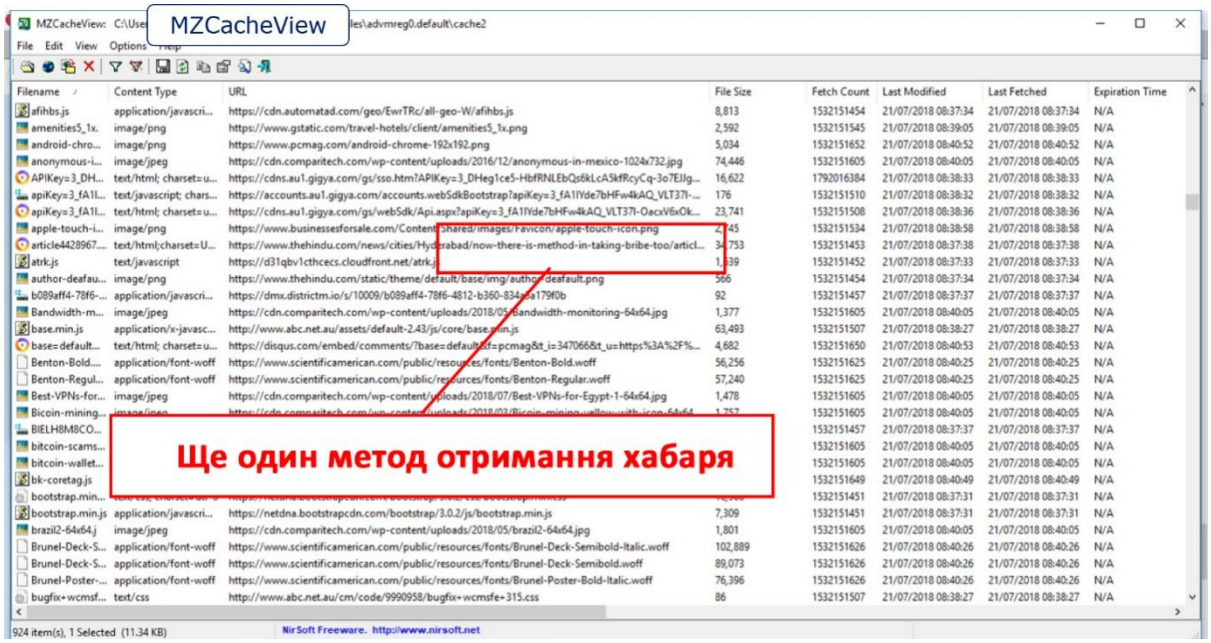
Якщо ввести в браузері about:cache, він покаже, які сайти ви переглядали і коли.

Функції кешування існують як відлуння тих часів, коли Інтернет був набагато повільнішим. Веб-сторінки, які Ви відвідали, зберігалися локально упродовж певного часу, тому якщо Ви знову забажаєте відвідати ту саму сторінку, комп'ютер спочатку перевірить, чи має він копії цієї веб-сторінки на своєму комп'ютері, а потім перевірить наявність будь-яких змін. Якщо змін не було, збережена (або «кешована») копія буде завантажена в браузер замість того, щоб чекати її завантаження. Сучасні швидкості Інтернету дають змогу обходитися без цього, але комп'ютер все ще здійснює ті самі дії.

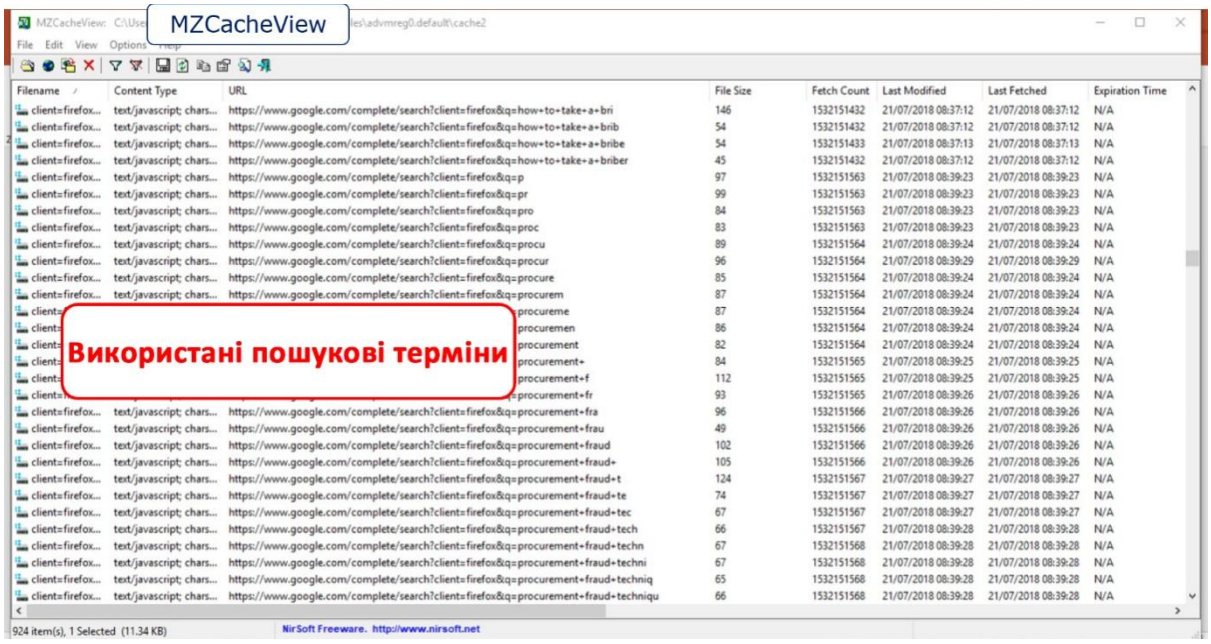
Посилання в кеші можуть містити безліч невідповідних відомостей, попри це, якщо уважно придивитись, то Ви можете побачити деталі, що становлять інтерес.



Пошук може полегшити використання програмного засобу для фільтрування інформації про кеш . На цих скріншотах зображено використання програми MZCacheView:



На цьому скріншоті показані пошукові терміни, які користувач застосовував на сайті Google.com: «Як взяти хабар» та «фальсифікація закупівель»:



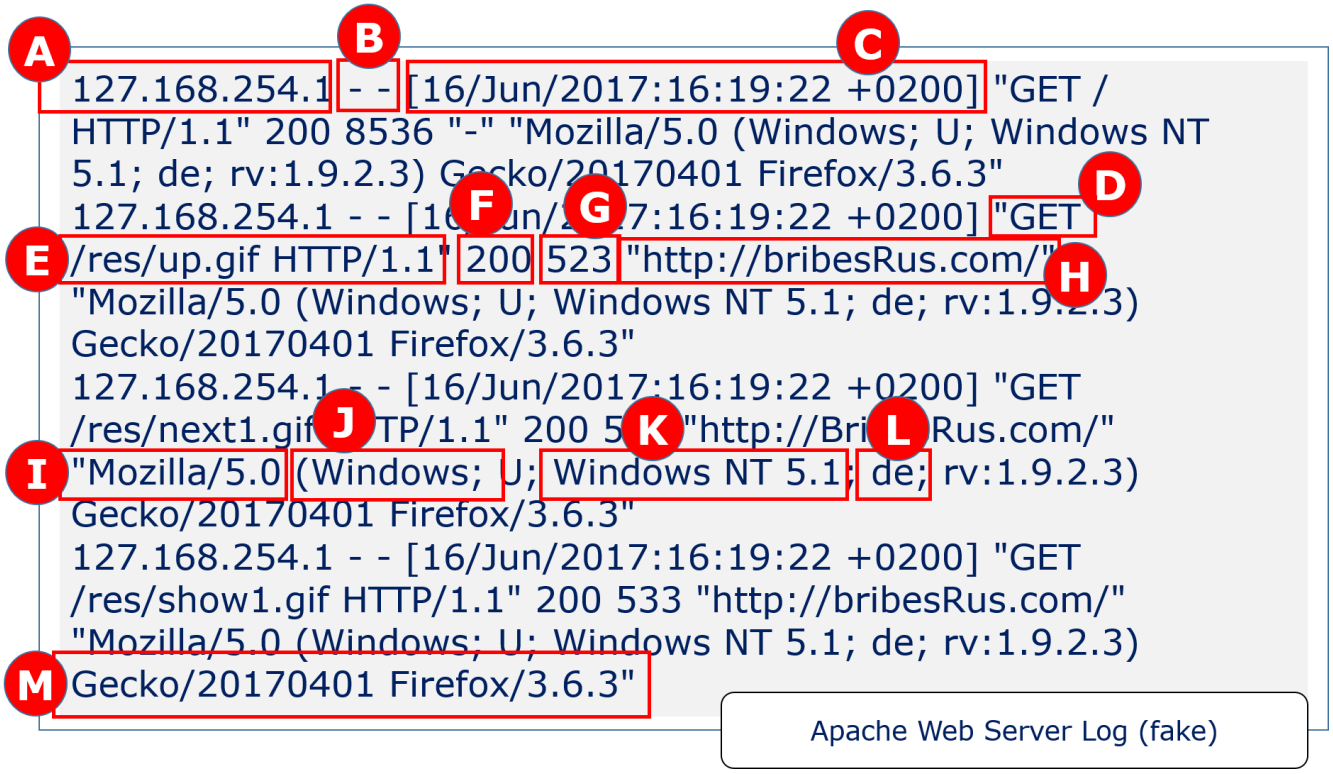
Якщо настройки не змінювалися, інтернет-браузер запише все, що шукав і проглядав користувач.

8.9 Журнали веб-серверів

Якщо інформація про пошук в Інтернеті не може бути знайдена на пристрої, слідчий може запитати інформацію з журналу веб-сервера. Вочевидь, це менш зручно і передбачає інформування третіх сторін про розслідування, яке ви, можливо, хотіли би тримати в секреті на даний момент. Однак це практичний варіант. У наступному прикладі було

зроблено копію реального журналу сервера, але всі дані, такі як IP-адреса та веб-сайти, були замінені на несправжні. [52]

З цього невеликого витягу журналу веб-сервера ви можете побачити величезну кількість інформації, яка може бути отримана. Він містить не тільки IP-адресу користувача, але і те, що користувач читав, коли це було, в якому часовому поясі, і яка мова при цьому використовувалася, а також те, яка операційна система працює на комп'ютері (однак цим можуть скористатися люди, які знають, як вивести до помилкового сліду, використовуючи комп'ютер).



Будь ласка, використовуйте клавішу нижче, щоб прочитати журнал.

Ключ журналу веб-сервера	
A	IP-адреса користувача
B	Ім'я користувача та логін (якщо не потрібно, то замінюється на –)
C	Часовий пояс – зауважте, що зазначаються години, хвилини та секунди, а також відхилення від GMT на +2 години

[52] Будь-який збіг з реальними даними є ненавмисним і абсолютно випадковим.

D	Це запит, надісланий вашим браузером на веб-сайт. GET означає, що файл є запитом. POST означає, що ви хочете завантажити або вставити дані на веб-сторінці
E	Це файловий шлях, що показує, де зберігається запитуваний файл
F	Це код результату. 200 означає, що запит був успішним. 404 означає, що він був невдалим.
G	Це розмір файлу в байтах
H	Це веб-сайт, на якому розміщений файл, що запитується
I	Тип браузера (Mozilla)
J	Програмна платформа на пристрої, що запитуєтеся
K	Версія операційної системи (Windows NT 5.1 означає Windows XP)
L	Мова браузера (de = німецька)
M	Версія браузера (Firefox), яка використовується

8.10 Дані з Exchangeable Image Format (EXIF)

Всі різні типи цифрових фотографій мають дані, за замовчуванням вбудовані в файл зображення. Стандарт називається Exchangeable Image File Format або EXIF. Дані Exif містять інформацію про параметри камери, які корисні для фотографа. Однак для доказових цілей вони розкажуть дату та час, коли була зроблена фотографія, марку та модель камери, а також серійний номер камери. Якщо підозрюваний був особливо недбалим, він навіть міг ввести своє ім'я в налаштуваннях камери, і це також буде показано. У дослідженні, де фотографії є частиною доказів, ви можете знайти підозрюваного за типом камери та порядковим номером, зазначеним у даних EXIF, тому це може бути дуже корисним.

Єдина засторога – дата та час на даних EXIF залежать від дати та часу, введеного в камеру. Якщо це не було зроблено належним чином (наприклад, дані за замовчуванням не були змінені), або якщо налаштування часу навмисно були змінені, реальний час буде відрізнятися від часу в EXIF.

Існує ще одна потенційно корисна властивість, про яку слід знати. Якщо цифрове зображення було зроблено за допомогою пристрою, в якому було увімкнено GPS, також імовірно, що координати GPS будуть міститися у даних EXIF.

Дані EXIF можуть бути видалені, включно із даними GPS. Раніше фотографії, завантажені на сторінки соціальних мереж, містили також дані EXIF, однак більшість, якщо не всі соціальні медіа, тепер знімають дані з зображення під час завантаження.

При цьому дані EXIF у завантажених зображеннях часто не враховуються.

Це схоже на те, що сталося з Джоном МакАфі, засновником компанії Internet Security Giant, що носить його ім'я. МакАфі продав власний бізнес і оселився в Белізі, проте він мав складні взаємини з місцевою владою. У 2012 році він підозрювався у вчиненні злочинів, пов'язаних з наркотиками та зброєю, але йому ніколи не висувалися звинувачення. Коли його сусіда, також американця, було знайдено вбитим, підозри впали на МакАфі, і правоохоронні органи прагнули допитати його, але він зник.

Хоча його перебування досі було невідоме, МакАфі дав інтерв'ю виданню Vice Magazine, і він дозволив сфотографувати себе на iPhone 4s. Коли історія згодом була завантажена на веб-сайт Vice.Com, вона була проілюстрована цією фотографією, що містила GPS-дані. Координати GPS вказують на те, що фотографія була зроблена в сусідній Гватемалі біля міста Ріо-Дульсе (місто в трьох годинах від Белізу, що відоме як дорогий курорт та місце відпочинку і проживання на пенсії).

МакАфі ніколи не переслідувався за вчинення злочинів, але його було депортовано, а його майно – конфісковано (його будинок незабаром після цього був спалений дотла).

Цифрові зображення, зроблені пристроєм з увімкненим GPS, зазвичай позначаються координатами місця та іншою корисною інформацію у форматі EXIF.

8.11 Електронні листи

Електронні листи можуть містити значні докази. Вони можуть зберігатися на пристрої, але частіше вони зберігаються на поштових серверах або у хмарі. Переважно, ми бачимо тільки найкоротші подробиці про те, хто надсилає електронний лист, кому він був відправлений, в який час відправник вирішив надіслати листа, чи написав він щось в темі листа, і якщо так – то що саме. Але електронні листи містять приховані дані у елементі, що називається заголовком електронної пошти.

Заголовок електронного листа може містити таку інформацію:

- Оригінальна IP-адреса, яку використав відправник;
- Обліковий запис електронної пошти відправника;
- Дата, час та IP-адреси серверів, через які він був маршрутизований;
- Інші процеси (наприклад, сканування антивірусу, або якщо шаблони в тексті вказують на потенційне шахрайство із застосуванням фішингу).

За замовчуванням під час перегляду електронної пошти Ви не можете бачити заголовок, але його досить легко знайти.

У Gmail:

У правому верхньому куті панелі повідомлень натисніть на маленьку стрілку вниз, щоб відкрити меню параметрів. Виберіть «Показати оригінал»

У програмі Hotmail або Outlook mail:

Також у правому верхньому куті повідомлення (поруч із кнопкою відповіді) відкрийте меню зі стрілкою вниз та виберіть «Перегляд джерела повідомлень».

Останні записи журналу з'являються у верхній частині заголовка, тому вони зчитуються знизу вгору. Однак зверніть увагу на те, що записи в заголовку можна підробити.

Дуже корисну вступну статтю про заголовки електронної пошти Джейсона Фолкнера можна знайти на сайті How-To Geek за посиланням:

https://www.howtogeek.com/108205/htg-explains-what-can-you-find-in-an-email-header/

Також зважайте на те, що налаштування облікового запису електронної пошти за допомогою несправжнього імені є абсолютно нескладним. Перевірки безкоштовних веб-служб електронної пошти щодо цього, зазвичай, є мінімальними і обійти їх дуже легко. Заголовки у безкоштовних веб-провайдерах електронної пошти використовують загальні сервери з загальними IP-адресами, однак правоохоронці можуть вимагати будь-яких відомостей про власника облікового запису.

Спектр інформації, яка доступна в обліковому записі, є великим та може включати:

- Ім'я власника рахунку
- Адреси власників рахунків
- Номер соціального страхування власника рахунку (у США)
- Платіжні адреси, пов'язані з обліковим записом
- Номери телефонів, пов'язані з обліковим записом
- Контактні імена
- Поштовий індекс
- Країна
- Пов'язані адреси електронної пошти
- Дата створення рахунку
- (Якщо є) Час закриття
- Усі IP-адреси та кожен логін
- MAC-адреси для маршрутизатора та будь-яких пристроїв, що використовувалися
- Загальна історія облікових записів
- Історія операцій: час, дата, кількість, типи

- Фінансові інструменти, що використовуються власником рахунку

8.12 Інструменти цифрової криміналістики

На завершення цього розділу, варто відзначити деякі цифрові криміналістичні варіанти програмного забезпечення (деякі з яких вже згадувалися мимохідь). Існує ціла низка високоякісних комерційних готових продуктів, що вражають уяву, включно із:

- EnCase від Guidance Software
- The Forensic Toolkit (FTK) від AccessData
- Electronic Evidence Examiner від the Paraben Corporation
- Celebrite, спрямований на смартфони та мобільні пристрої

На жаль, ліцензії на комерційні продукти можуть бути надзвичайно дорогими, але за ці гроші вони пропонують повну підтримку та навчання. Проте ліцензії означають, що значний рівень поточних інвестицій є необхідним, і цей рівень інвестицій не відповідає бюджету правоохоронних органів багатьох країн.

Існує також програмне забезпечення з відкритим кодом, яке називається Sleuthkit (TSK) та Autopsy. Воно безкоштовне та розроблено талановитими аматорами, які жертвують власними навичками для більшого добра криміналістики, але для цього потрібні трохи більше технічних знань, ніж для комерційних аналогів.

Список популярних інструментів можна знайти тут:

https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

На додаток до готових продуктів, кваліфіковані програмісти завжди можуть створювати свої власні програмні засоби, але це вимагає жорсткого тестування та перевірки, щоб не виникли проблеми, схожі на ті, що виникли у справі Кейсі Ентоні.

Важливо зазначити, що немає кнопки «докази». Програмне забезпечення не може робити висновки, воно може перетворити результати лише на конкретні запити залежно від того, яка інформація була надана. Експерт-криміналіст повинен бути кваліфікованим та достатньо обізнаним, щоб зробити точні висновки з результатів програмного забезпечення та вміти пояснювати суду, чому він/вона досягла цих висновків.

Питання для перевірки знань:

1. Як гарантується цілісність копії диска?
2. Як ви отримуєте інформацію з Інтернет-браузера?
3. Чому небезпечно розміщувати зображення безпосередньо в Інтернеті?

Вивчення та огляд:

Використовуючи інформацію в цьому розділі, перегляньте наявні дані на своєму комп'ютері, зокрема: історію переглядів, EXIF-дані на цифровій фотографії та заголовок електронного листа.

9 ОСНОВНІ ЗАСАДИ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В УКРАЇНІ

Як виявилось, нові та прогресивні норми про електронні докази та їх застосування в судовому процесі України в певній частині виявились занадто складними та нежиттєздатними на практиці.

Перш за все визначимо, про які докази йдеться. Це питання має також і прикладне значення, оскільки стосується обов'язкових реквізитів та вимог, які ставляться до цих доказів.

Поняття «електронні докази» з'явилося ще в 70-х роках XX ст. з появою так званих машинних документів. У світовій практиці існує термін data message, що в ст.2 Типового закону про електронну торгівлю від 1997 року, рекомендованого Генеральною Асамблеєю ООН, визначається як інформація, що підготовлена, відправлена, отримана або збережена за допомогою електронних, оптичних або аналогічних засобів, включаючи електронний обмін даними, електронну пошту, телеграф, телекс або факс. Якщо говорити про міжнародний досвід, то в Німеччині сила електронних доказів підкріплюється електронним цифровим підписом. У Франції ж електронні документи мають таку ж саму юридичну силу, як і паперові, вони підписуються й не потребують зв'язку з конкретним технологічним засобом. Електронні документи визнавалися доказами і в багатьох рішеннях Європейського суду з прав людини, зокрема у справах «P. and S. v. Poland» (від 30.10.2012), «Eon v. France» (від 14.03.2013), «Shuman v. Poland» (від 3.06.2014).

У національному праві юридичну значущість електронного документа закріпили при прийнятті Цивільного кодексу, а також у законах «Про електронні документи та електронний документообіг» від 22.05.2003 №851-IV та «Про електронні довірчі послуги» від 05.10.2017 №2155-VIII (набув чинності 07.11.2018 р.)

Відповідно до ч.1 ст.5 закону №851-IV електронним вважається документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. На практиці як такий вид доказів можуть використовуватись аудіо-, відеозаписи, документи бухгалтерської та податкової звітності, що створені, передані, отримані в електронній формі, роздруківки інтернет-сторінок, СМС-листування, листування електронною поштою, публікації в соціальних мережах тощо.

9.1 Електронні докази: поняття, види

Електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет).

Електронні докази подаються в оригіналі або в електронній копії, засвідченій електронним цифровим підписом, прирівняним до власноручного підпису відповідно до Закону України " Про електронні довірчі послуги". Законом може бути передбачено інший порядок засвідчення електронної копії електронного доказу.

Учасники справи мають право подавати електронні докази в паперових копіях, посвідчених у порядку, передбаченому законом. Паперова копія електронного доказу не вважається письмовим доказом.

Учасник справи, який подає копію електронного доказу, повинен зазначити про наявність у нього або іншої особи оригіналу електронного доказу.

Якщо подано копію (паперову копію) електронного доказу, суд за клопотанням учасника справи або з власної ініціативи може витребувати у відповідної особи оригінал електронного доказу. Якщо оригінал електронного доказу не подано, а учасник справи або суд ставить під сумнів відповідність поданої копії (паперової копії) оригіналу, такий доказ не береться судом до уваги.

Електронні документи: чи обов'язковий ЕЦП?

Як відомо, правовий режим електронних документів регулюється спеціальним законом, в якому зазначається, що електронним документом є документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

У ст. 6 Закону України "Про електронні документи та електронний документообіг" передбачається можливість застосування електронного підпису для ідентифікації автора документа, однак ця вимога не є обов'язковою.

Водночас колізія виникає, якщо проаналізувати ст. 7 цього Закону, де зазначається, що оригіналом електронного документа є електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного в розумінні Закону України " Про електронні довірчі послуги ".

Звідси буквальне тлумачення положень закону приводить до висновку, що електронні документи, які не посвідчені ЕЦП, можуть вважатись електронними документами, однак не будуть вважатись оригіналами таких документів в розумінні цього Закону, що є очевидно суперечливим.

Незрозумілість виникає також після аналізу ч. 2 ст. 6 згадуваного Закону, згідно з якою саме накладанням електронного підпису завершується створення електронного документа.

Зауважимо, що раніше (до 06.11.2014 року) ч. 1 ст. 6 цього Закону закріплювала наявність електронного підпису як обов'язкового реквізиту для електронних документів. Як бачимо, внесені в 2014 році зміни до профільного Закону були вибірковими, що породило низку колізій, які в даному випадку впливають на розуміння обсягу поняття електронні документи.

Як вбачається із проаналізованого законодавства, то слід керуватись ст. 7 цього Закону та вважати наявність електронного підпису необов'язковою вимогою для електронних документів з метою можливості їх використання в судовому процесі у якості належних та

допустимих доказів. Посвідчення електронним підписом електронних документів (крім текстового документа) є досить складною процедурою, якою не володіють навіть більшість професіоналів-програмістів. До того ж законодавством не передбачається навіть процедура перевірки ЕЦП судами при поданні електронних доказів. Як наслідок, ставиться під сумнів доцільність закріплення такої занадто ускладненої процедури подання до суду цього засобу доказування.

9.2 Особливості регулювання у КПК

Окремо слід звернути увагу на те, що в діючому КПК України відсутнє поняття електронного документу і відсутня окрема норма, яка б регулювала поводження з електронними доказами. В свою чергу, ст.99 КПК "Документи", містить загальні положення про поводження з документами, як доказами.

Ч.1 ст.99 КПК України визначає документ як спеціально створений з метою збереження інформації об’єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

Тобто, діючий КПК України, не виділяє окремо поняття електронного документу, однак вказує, що документом, за певних умов, може вважатись об’єкт, який містить в собі оцифровану, звукову чи візуальну інформацію.

Згідно п.1 ч.2 ст.99 КПК України визначено, що: До документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні).

Отже, дана норма виділяє електронні носії інформації окремо, і окремо носії відео та звукової інформації (яка не є електронною інформацією). Наприклад, це може бути відео, аудіокасета із записом тощо… і КПК України визначає це як документ. Натомість, КАС, ГПК та ЦПК України не вважають такі об’єкти документами, а, скоріше за все, це будуть речові докази, оскільки під поняття письмових доказів вони не підпадають, а узагальнююче поняття документу у вищезгаданих кодексах відсутнє.

9.3 Електронні документи

Для того, щоб виділити електронний документ з маси всіх інших електронних документів, він повинен бути певним чином персоніфікований, тобто наділений особливими атрибутами, за якими надалі може бути здійснена його ідентифікація. Роль персоніфікуючих атрибутів електронного документа виконують його реквізити, до яких відносяться: 1) ім'я файлу, яке присвоюється йому цілеспрямовано творцем інформації або автоматично без його волі; 2) формат файлу, який визначається програмним забезпеченням, за допомогою якого він був створений або збережений; 3) розмір файлу, який становить собою обсяг пам'яті машинного носія, який займає файл; 4) дата і час створення або редагування файлу.

Крім персоніфікуючих реквізитів, електронний документ може містити захисні або посвідчувальні реквізити. Наприклад, одним з реквізитів електронного документа, який одночасно є персоніфікуючим і захисним, можна назвати електронний підпис

(електронний цифровий підпис). Відповідно до Закону України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV, під ЕЦП розуміється «вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа».

Закон України "Про електронні документи та електронний документообіг":

Стаття 8.

Правовий статус електронного документа та його копії

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Для того щоб виділити електронний документ з маси всіх інших електронних документів, він повинен бути певним чином персоніфікований, тобто наділений особливими атрибутами, за якими надалі може бути здійснена його ідентифікація. Роль персоніфікуючих атрибутів електронного документа виконують його реквізити, до яких відносяться: 1) ім'я файлу, яке присвоюється йому цілеспрямовано творцем інформації або автоматично без його волі; 2) формат файлу, який визначається програмним забезпеченням, за допомогою якого він був створений або збережений; 3) розмір файлу, який становить собою обсяг пам'яті машинного носія, який займає файл; 4) дата і час створення або редагування файлу.

Крім персоніфікуючих реквізитів, електронний документ може містити захисні або посвідчувальні реквізити. Наприклад, одним з реквізитів електронного документа, який одночасно є персоніфікуючим і захисним, можна назвати електронний підпис (електронний цифровий підпис). Відповідно до Закону України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV, під ЕЦП розуміється «вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних

даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа».

Електронний документ не може існувати без носія інформації. При цьому, мають значення, що ідентифікують ознаки носія інформації, які включають найменування типу, марки, моделі, індивідуального серійного номера і т.п. машинного носія, на якому записаний файл.

Важливе значення при дослідженні електронних документів має проблема встановлення достовірності електронних доказів і забезпечення їх доказової сили. На сьогодні в процесуальному законодавстві не передбачені конкретні критерії достовірності електронних доказів.

Правила забезпечення достовірності електронних доказів і пред'явлення їх в суді.

Наразі на практиці склалися деякі правила забезпечення достовірності електронних доказів і пред'явлення їх в суді:

1) якщо електронний документ містить в собі графічну або текстову інформацію, то роздруковується його паперова копія, яка оформлюється і завіряється уповноваженою особою; така копія долучається до справи і досліджується як звичайний письмовий документ;

2) якщо операції, що документально підтверджуються електронним документом (електронний документ підписаний ЕЦП), а сторони не визнають надання послуг, що підтверджуються цим документом, то призначається комплексна експертиза, де економічна експертиза проводиться вже за даними щодо автентичності ЕЦП;

3) якщо електронний документ являє собою сторінку в мережі Інтернет, то така сторінка за умови посилання роздруковується на папері, оформляється і завіряється як копія веб-сторінки при зверненні зацікавленої особи; завірений роздрук сторінки сайту долучається до справи та досліджується в процесі;

4) якщо електронний документ несе в собі аудіо- або відеоінформацію, то, як правило, робиться копіювання таких файлів на окремий переносний електронний носій, який долучається до справи та досліджується за допомогою спеціальних технічних засобів.

Таким чином, для того щоб визнати електронні документи в якості повноцінних достовірних доказів, необхідно суворо дотримуватися правил процесуального законодавства, а також стандартних прийомів і методик збирання, оцінки, дослідження та використання електронних доказів. Лише в цьому випадку зацікавлена особа зможе розраховувати на прийняття судом та, своєю чергою, експертом - економістом до уваги подібних документів

9.4 Веб-сайти (сторінки)

Перший у світі сайт info.cern.ch з'явився в 1990 році. Його створив Тім Бернерс-Лі — батько сучасного інтернету. Автор опублікував на своєму сайті опис нової технології WWW (World

Wide Web), заснований на протоколі передачі даних HTTP, системі адресації URI і мові розмітки HTML. Також на ресурсі було описано принципи встановлення та роботи серверів і браузерів. Сайт став першим у світі інтернет-каталогом, на якому Тім Бернерс-Лі розмістив гіперпосилання на інші інтернет-ресурси, що розпочали своє існування.

Web-сервер — це комп'ютер з набором спеціальних програм, що забезпечують доступ до даного комп'ютера через Інтернет, що містить файли, складові наповнення web-сайта. Web-сторінка — самостійна частина web-сайта, що представляє собою документ, забезпечений унікальною адресою.

Назва пояснюється тим, що кожна сторінка, що відображається на моніторі, асоціюється з газетною сторінкою, У зв'язку з цим web-сайти зазвичай мають рекомендовану ширину для перегляду на екрані комп'ютера. Втім, сторінка може бути і набагато більша, ніж розмір екрану. В такому випадку для її відображення використовуються допоміжні функції Web-браузера — смуги прокрутки. Web-сайти сформовані з великої кількості сторінок. Одна зі сторінок web-сайту, як правило, є головною або первісною (її називають Home Page — домашня сторінка). Це свого роду відправна точка всього сайту, з якої йдуть посилання на інші сторінки.

Для професіонала web-сайт являє собою документ, створений за допомогою певної мови програмування або мови розмітики наприклад HTML, PHP, ASP, JAVA, доступний користувачеві за допомогою протоколу HTTP, який передає інформацію від web-сервера до web-браузера (наприклад, Microsoft Internet Explorer або Google Chrome).

Протокол становить собою письмовий набір директив, які визначають, як два комп'ютери можуть зв'язатися один з одним, дотримуючись єдиних стандартів.

Очевидно, що web-сайт повинен бути доступний з будь-якого пристрою, який використовує протокол HTTP, наприклад: комп'ютера, мобільного телефону, кишенькового персонального комп'ютера (КПК) і т.д.

Структури web-сайтів надзвичайно різноманітні і визначаються цілями, бажаннями і можливостями особи, що розміщує інформацію. Крім того, при розробці web-сайту необхідно брати до уваги, якій конкретно аудиторії цей сайт призначений. Залежно від цього ми можемо задати умови, які будуть покладені в основу створюваного проекту. Приміром, якщо сайт — це пошукова система або сторінка курсів валют, то очевидно, що сайт повинен бути якомога меншим і використовувати прості технології для полегшення завантаження з будь-якого пристрою.

Веб-сайти бувають 2 типів: статичні і динамічні.

Статичний web-сайт складається з статичних web-сторінок, які створюються вручну, потім зберігаються і завантажуються на сайт. Їх вміст досить постійний і міняється досить рідко. Кожного разу, коли потрібно змінити вміст такої сторінки, програміст або web-майстер модифікує її на робочому комп'ютері, зберігає і потім заново завантажує на web-сервер.

Сайт, розроблений за допомогою мови HTML (HyperText Markup Language — мова розмітки гіпертексту — стандартна мова для створення web-сторінок), є web-сайтом статичного типу і складається з декількох статичних сторінок.

Динамічний web-сайт — це система, готова до інформаційного оновлення. Він заснований на шаблонних сторінках, в які вставляється постійно змінне інформаційне наповнення, яке зберігається зазвичай у базі даних. На сторінці після запиту користувачем відповідна інформація витягується з бази, вставляється в шаблон, утворюючи нову web-сторінку, і пересилається web-сервером в браузер користувача, який і відображає її належним чином. Отже, для оновлення вмісту динамічного сайту достатньо просто додати текст для нової сторінки, який потім буде вставлений в базу даних за допомогою певного механізму. Іншими словами, web-сайт наче оновлює себе сам. Наповнювати іформацією динамічний сайт може людина без спеціалізованих знань програмування або HTML-коду.

9.5 Проблеми фіксації інформації як доказу в мережі Інтернет

Забезпечення збору та фіксації доказів в мережі Інтернет є наріжною проблемою захисту авторських прав, оскільки в цифровому середовищі обмін інформацією та використання творів відбувається набагато стрімкіше, ніж в інших. З моменту порушення і до моменту судового розгляду інформація, що міститься на певній веб-сторінці, може бути неодноразово змінена чи взагалі така веб-сторінка перестане існувати.

Основною метою фіксації певної інформації є отримання належних і допустимих доказів, які потім можуть бути використані в суді. Водночас, нібито легко зрозуміле завдання допоки так і не знайшло належного розв'язання в Україні ані на рівні законодавчого регулювання, ані на рівні правозастосовної практики. Наприклад, законодавством не встановлений перелік способів фіксації змісту веб-сторінок в мережі Інтернет, не розв'язані інші питання.

Крім того, аналіз норм законодавства та наукових поглядів дає підстави запропонувати класифікацію способів фіксації змісту веб-сторінки в мережі Інтернет, що може становити користь у процесі правозастосування. Так, за особою, яка проводить фіксацію змісту сторінки в мережі Інтернет, може розрізнятися: фіксація, що проводиться самостійно правоволоділець (чи його представником); фіксація, яку здійснюють треті особи (нотаріуси, судові експерти, патентні повірені, постачальники посередницьких послуг); фіксація, яку здійснює суд.

У свою чергу за характером фіксації можуть використовуватися наступні способи фіксації: візуальні (за яких здійснюється лише візуальний огляд зображення, яке подається на екран пристрою виведення інформації) та технологічні.

Візуальні способи фіксації:

1) Роздруківка веб-сторінки (Web-скріншот).

Відповідно до п. 46 Постанови Пленуму ВГС України від 17.10.2012 р. № 12 роздруківки Інтернет-сторінок (web-сторінок) самі по собі не можуть бути доказом у справі. Втім, матеріали судової практики свідчать про визнання такої роздруківки як доказу за умови відсутності заперечень від інших осіб, що беруть участь у справі. Так, Апеляційний суд м. Києва у справі № 22-9597 встановив, що факт використання твору був доведений позивачем шляхом надання суду письмового доказу – копії роздруківки сторінки з належного відповідачу сайту forum.com.ua, яка містить кольорове зображення твору образотворчого мистецтва – карикатури під назвою "Кан-кан". Відповідно до положень

цивільного процесуального законодавства, якщо при дослідженні письмових доказів особою, яка бере участь у справі, буде подана заява про те, що доданий до справи або поданий іншою особою для ознайомлення документ викликає сумнів з приводу його достовірності або є фальшивим, особа, яка подала цей документ, може просити суд виключити його з числа доказів і розглядати справу на підставі інших доказів. При відсутності з її боку таких процесуальних дій, особа, яка подала заяву, має згідно із загальними правилами доказування подати відповідні докази, що спростовують значення відомостей оспорюваного документа і могли бути підставою неприйняття його до уваги під час оцінки доказів. У даному випадку відповідач не надав суду жодного доказу на спростування значення відомостей, які містяться на роздруківці сторінки з належного відповідачу сайту forum.com.ua, що містить кольорове зображення твору образотворчого мистецтва – карикатури під назвою "Кан-кан". За таких обставин у суду немає підстав вважати, що факт використання твору шляхом розміщення твору образотворчого мистецтва на сайті не є доведеним.

2) Фіксація особою контенту, шо міститься на веб-сайті, шляхом його збереження на відповідних носіях (CD, DVD, магнітні диски тощо). Від попереднього способу відрізняється лише об'єктивною формою існування результатів фіксації. За своєю суттю так само становить фактично роздруківку веб-сторінки.

3) Протокол огляду веб-сторінки нотаріусом. Згідно зі ст. 75 ЗУ «Про нотаріат» нотаріус та посадові особи органів місцевого самоврядування, які вчиняють нотаріальні дії, можуть засвідчувати вірність копій документів, виданих підприємствами, установами і організаціями. Однак чи є web-скріншот таким документом? Слід погодитися з думкою, що ці об'єкти не можна ототожнювати, «оскільки подібні документи повинні містити найменування суб'єкта господарювання, дату, підпис уповноваженої особи, а в деяких випадках і печатку. Крім того, веб-сторінка не завжди містить посилання на суб'єкт, який використовує інтернет-сайт».

Станом на вересень 2017 р. українські нотаріуси відмовляють у здійсненні протоколу огляду веб-сторінки через відсутність такої нотаріальної дії у ЗУ «Про нотаріат» та в Порядку вчинення нотаріальних дій нотаріусами України.

Втім, відповідно до ст. 6. Угоди «Про порядок вирішення спорів, пов'язаних із здійсненням господарської діяльності» від 20.03.1992 р., сторонами яких є Україна, Білорусь і Російська Федерація, документи, які на території однієї з Договірних Сторін видані або засвідчені компетентною установою або спеціально на те уповноваженою особою в межах його компетенції та за встановленою формою і скріплені гербовою печаткою, приймаються на територіях інших Договірних Сторін без будь-якого спеціального посвідчення.

Так, відповідно до ст.ст. 102, 103 «Основ законодавства про нотаріат» Російської Федерації нотаріус на прохання зацікавлених осіб забезпечує докази, необхідні у разі виникнення справи в суді або адміністративному органі, якщо є підстави вважати, що подання доказів згодом стане неможливим або складним. Огляд веб-сайту нотаріусом РФ складається з наступних етапів: перевірка доменного імені, встановлення DNS-серверів; перевірка відповідності IP-адреси; перевірка достовірності відображення вмісту веб-сайту з тим, до якого звертається браузер; відображення переходів на сторінки, які цікавлять заявника. Кожен етап фіксується в описовій частині протоколу, результати огляду (веб-сторінки,

фотографії, скріншоти) роздруковуються і підшиваються до протоколу . Крім того, в протоколі зазначається опис оглянутих веб-сторінок, зміст доказів, місце та час вчинення нотаріальної дії, відомості про зацікавлених осіб та нотаріуса .

Зазначимо, що згідно з ч. 2. ст. 96-2, ст. 96-4 Закону Республіки Білорусь «Про нотаріат і нотаріальну діяльність» нотаріуси республіки Білорусь наділені повноваженнями із забезпечення письмових доказів, а інформація, розміщена в мережі Інтернет та отримана в результаті проведення нотаріусами огляду інтернет-сторінок, відноситься до письмових доказів.

Результати огляду письмового доказу фіксуються нотаріусом шляхом складання протоколу огляду письмового доказу. Такий протокол має містити: дату, час (години, хвилини) і місце проведення огляду; інформацію про особу, що здійснює огляд (його прізвище та ініціали, статус (нотаріус), найменування нотаріального округу); відомості про осіб, присутніх при огляді; зміст заяви особи, яка звернулася за вчиненням нотаріальної дії, із зазначенням причин, в силу яких представлення доказів стане згодом неможливим або складним; послідовність дій нотаріуса з приводу огляду такої інформації. До протоколу огляду можуть долучатися роздруковані на паперовому носії зображення інформації, опублікованої на сторінках інформаційного ресурсу, а також зображення на паперовому носії, що відображають послідовність виробництва нотаріусом дій по доступу до цієї інформації. У разі залучення до протоколу роздрукованих на паперовому носії зображень інформації в протоколі вказується час (години, хвилини), коли була проведена роздруківка цієї інформації. На прохання особи, яка звернулася за вчиненням нотаріальної дії, до протоколу огляду письмового доказу може долучатися електронна версія оглянутих доказів.

4) Огляд доказів судом за їх місцезнаходженням. Відповідно до положень ст. 85 ЦПК України та ст.82 ГПК України речові письмові та електронні докази, які не можна доставити в суд, оглядаються за їх місцезнаходженням. Суд за заявою учасника справи чи з власної ініціативи може оглянути веб-сайт (сторінку), інші місця збереження даних в мережі Інтернет з метою встановлення та фіксування їх змісту. У разі необхідності для проведення такого огляду суд може залучити спеціаліста. За результатами огляду та дослідження суддею складається відповідний протокол.

5) У п.46 Постанови Пленуму ВГС України від 17.10.2012 № 12 також вказується на можливість проведення відео-, аудіозапису процесу дослідження будь-якою заінтересованою особою сайту, стосовно якого є відомості використання його з порушенням авторських чи суміжних прав. Такий запис, здійснений на електронному чи іншому носії (жорсткому диску комп'ютера, дискеті, диску для лазерних систем зчитування, іншому носії інформації), подається до суду із зазначенням того, коли, ким і за яких умов цей запис здійснено і може бути речовим доказом у справі.

6) Як окремий спосіб фіксації виділяють також проведення протоколу огляду веб-сайту адвокатом на підставі його професійного права на збирання відомостей про факти, що можуть бути використані як докази відповідно до п. 7 ч. 1 ст. 20 ЗУ «Про адвокатуру та адвокатську діяльність».

До технологічних спосіб фіксації (тобто таких, що приділяють увагу технічним аспектам функціонування веб-сторінок) слід віднести:

1) Довідки, отримані від провайдерів (log-файли). У зазначених файлах може міститись інформація щодо дій користувачів з приводу розміщення інформації. Однак, зміст такої інформації може різнитися в залежності від налаштувань хостингу. Крім того, такі файли фіксують тільки ім'я файлу, а не його зміст .

2) Миттєва фіксація веб-сторінок за допомогою приватних онлайн-сервісів. За такої фіксації здійснюється фіксація не тільки візуального відображення, а й вихідного коду, URL-адреси веб-сторінки та часу здійснення такої фіксації. Різновидом попереднього способу є фіксація за допомогою приватних онлайн-сервісів кешованої копії веб-сторінки у пошукових системах. Так, Т. Жуковський зазначає, що, «якщо з моменту видалення веб-сторінки минуло небагато часу, існує шанс, що вона збереглася у вигляді кешованої копії веб-сторінки, збереженої відповідною пошуковою системою у момент, коли пошуковик в останнє відвідував зазначену веб-сторінку». Втім, питання щодо належності і допустимості таких сервісів залишається дискусійним.

3) Використання сервісу InternetArchive. WaybackMachine, який здійснює фіксацію змісту окремих веб-сторінок як в автономному режимі, так і на вимогу користувача. Зазначений сервіс має статус бібліотеки і підпорядкований праву США. Існують певні технічні обмеження такої фіксації змісту веб-сторінки: так, не зберігаються об'єкти, розмір яких більше 10 МБ, не зберігаються сторінки з обмеженим доступом. Крім того, на вимогу власника веб-сайту дані з цього веб-архіву видаляються. Матеріали української судової практики у спорах про право інтелектуальної власності свідчать про залучення в якості доказів матеріалів судових експертиз, де предметом дослідження, зокрема, є згаданий сервіс, а не в якості окремих доказів.

Так, у рішенні від 24.09.2012 р по справі № 59/230 Господарський суд м. Києва зазначав, що позивач не погоджувався з висновком комплексної комісійної судової експертизи у сфері інтелектуальної власності, оскільки вважав, що інформація, отримана експертом за матеріалами веб-сайту www.archive.org є не точною, ненадійною та такою, що може не відповідати дійсності. Однак, позивач не надав суду доказів в підтвердження того, що інформація стосовно веб-сайту відповідача за відомостями веб-сайту www.archive.org є неправдивою та недостовірною . У рішенні Господарського суду м. Києва від 17.10.2016 р. по справі № 910/11186/16 щодо дострокового припинення дії свідоцтва України на знак для товарів і послуг судом було також оцінено матеріали експертного дослідження телекомунікаційних систем (обладнання) та засобів від 30.08.2016 р., в рамках якого досліджувалось та було зафіксовано наповнення веб-сторінок Інтернет-архіву «The Wayback Machine».

Матеріали судової практики в іноземних державах свідчать, що збережені копії Internet Archive визнаються судами в якості доказів в Російській Федерації та США .

4) Проведення експертного дослідження за експертизою 10.17 – дослідження телекомунікаційних систем (обладнання) та засобів.

За умови, якщо це потребує спеціальних знань і не може бути здійснено судом самостійно або із залученням спеціаліста, суд може призначити експертизу для встановлення та фіксування змісту веб-сайту (сторінки), інших місць збереження даних в мережі Інтернет.

При проведенні експертного дослідження у сфері телекомунікацій проводяться наступні дії: перевірка доменного імені (експерт встановлює, чи існує web-сайт із відповідним доменним ім'ям в мережі Інтернет на дату проведення дослідження та чи коректно здійснюється з'єднання з ним); фіксація редиректу на інше доменне ім'я (якщо таке має місце); фіксація даних, отриманих за допомогою сервісу WHOIS (експерт встановлює дані про дату реєстрації доменного імені, дату внесення останніх змін, про адміністратора домену); визначення IP-адреси, якій відповідає доменне ім'я; фіксація даних про компанію, що надає послуги хостингу для даного доменного імені; перевірка коректності відображення вмісту web-сайту; відображення головної сторінки; переходи на сторінки, на яких розміщені об'єкти інтелектуальної власності чи інформація, що мають значення для дослідження, та їх фіксація; фіксація аудіо, відео або текстових файлів, розміщених на web-сайті, що мають значення для дослідження (такого роду дослідження вкрай актуальні при порушенні авторських прав в мережі Інтернет); фіксація всього web-сайту, якщо це необхідно. Крім того, при проведенні даного експертного дослідження відбувається дослідження вихідного коду/тексту веб-сайту.

Наголосимо, що авторські права порушує не саме існування веб-сторінки, а розміщення в мережі Інтернет окремого твору (творів) у цифровій формі. Такі твори можуть і не розміщуватися безпосередньо на досліджуваних веб-сторінках, а розміщуватися, наприклад, у складі веб-банерів таргетингової реклами.

Візуальні способи фіксації не включають огляд вихідного коду веб-сторінки, що вкрай важливо для визначення, на якому саме веб-сайті відбувається використання твору (у випадках хотлінкінгу, фреймінгу та використання спеціалізованих тегів інтернет-розмітки, таких як <embed>, <object>, <video>, <audio>, <iframe>). Вважаємо, що при проведенні фіксації змісту веб-сторінки в мережі Інтернет обов'язково повинен аналізуватися (чи принаймні зберігатися) вихідний код веб-сторінки. Саме за допомогою вихідного коду можливо встановити, на якому веб-сайті розміщений відповідний твір, а відтак – визначити належного відповідача. Жодний з візуальних способів фіксації змісту веб-сторінок не в змозі дати належне і достовірне уявлення про те, що ж насправді розміщується (і чи розміщується) на даній веб-сторінці і чи не була вона модифікована, оскільки такий спосіб є лише відтворенням (останнім етапом використання твору в Інтернеті), яке подається на пристрій виведення інформації, а не дослідженням її внутрішньої структури (що здатне довести правомочності відтворення та надання твору до загального відома публіки). Крім того, таке відтворення може суттєво відрізнятися в залежності від програмного забезпечення, що використовується для проведення фіксації; версії операційної системи; роздільної здатності пристрою виведення інформації, тобто мати адаптивний дизайн, чи регіонального обмеження доступу до веб-ресурсу по IP-адресі; обмеження доступу до веб-ресурсу протягом певних годин доби тощо. Крім того, протокол огляду веб-сторінки нотаріусами не здатний зафіксувати факт наявності та використання музичних і аудіовізуальних творів.

9.6 Приклади справ

В адміністративній справі одним із основних доказів була роздруківка зображення та фотознімків зі сторінки в Facebook. Окружний адміністративний суд м. Києва зайняв сторону відповідача та Постановою від 14.12.2013 р. в справі №826/19865/13-а залишив позов без задоволення. Суд вказав, що позивачем не надано доказів, які б підтверджували, що сторінка у Facebook створена та підтримується саме відповідачем або його довіреними особами. Суд також зазначив, що в Facebook може зареєструватись будь-яка особа та під будь-яким іменем, відтак, створити та підтримувати сторінку відповідача, у тому числі шляхом розміщення інформації та фотознімків, могла будь-яка особа, встановити яку під час розгляду даної справи є неможливим (http://www.reyestr.court.gov.ua/Review/36029965).

У справі №2/463/169/14 рішенням Личаківського районного суду м. Львова від 15.01.2014 р. позивачам було відмовлено в позові про захист честі, гідності, відшкодування моральної шкоди, адже, на думку суду, вони не довели належними та допустимими доказами поширення винними діями відповідачів інформації в Інтернеті, зокрема, на сайті Twitter.

При цьому, відповідач категорично заперечила факт розповсюдження будь-якої інформації в Інтернеті та своє відношення до користувача під ніком «imya prizvyshche» на сайті Twitter. Оскільки позивач не надав будь-яких інших об'єктивних доказів поширення негативної інформації саме відповідачем, окрім як роздруківок інформації з Twitter, суд відмовив в позові з мотивів недоведеності (http://www.reyestr.court.gov.ua/Review/36711398).

В іншій справі №464/1324/14-ц, заперечуючи проти позову про захист честі, ділової репутації та відшкодування моральної шкоди, яка полягала у поширенні відповідачем неправдивої інформації у Одноклассники та Вконтакті, відповідач, обрав спосіб захисту та зазначив, що вказана позивачем інформація ним в жоден спосіб не поширювалась. Натомість, надані позивачем роздруківки із сторінки в соціальній мережі, яка створена під його іменем, не є допустимими доказами, оскільки їх дійсність неможливо перевірити.

У зазначених соціальних мережах будь-яка особа може створити сторінку під будь-яким іменем, а позивачем не надано жодних доказів того, що вказана інформація поширена саме відповідачем, оскільки ним така сторінка не створювалась, інформація не поширювалась. Саме на підставі недоведеності позовних вимог належними та допустимими доказами Сихівський районний суд міста Львова рішенням від 03.04.2014 р. відмовив позивачу в задоволенні позову (http://www.reyestr.court.gov.ua/Review/38252647).

На фоні цих рішень винятком є Постанова Київського апеляційного адміністративного суду у справі №2а-13438/12/2670 від 21.02.2013 р., якою позов задоволено і в якості належних доказів суд прийняв прінт-скріни (фотознімки екрану монітору користувача) сторінок в Facebook та Twitter. Основним аргументом суду на користь прийняття таких матеріалів в якості доказів було те, що зробити такі прінт-скріни могла лише визначена особа, що мала необхідні ключі для входу до адміністративної частини сайту(http://www.reyestr.court.gov.ua/Review/29649736).

Рішення Дрогобицького міськрайонного суду Львівської області від 27.03.2014 р. у справі №442/1484/14-ц. Суд дійшов висновку, що між сторонами спору укладено договір шляхом обміну електронними листами (перепискою Вконтакті) і грошові кошти перераховані відповідачу в якості оплати за цим договором. Суд прирівняв листування між акаунтами

ВКонтакті до електронних листів, що в свою чергу є підтвердженням досягнення між сторонами письмової згоди про укладення договору (абзац другий ч. 1 ст. 207 ЦКУ).

Відповідач не заперечував факту ведення саме ним вказаного листування і не оскаржував рішення суду в апеляційному порядку (http://www.reyestr.court.gov.ua/Review/38011009).

9.7 Текстові, мультимедійні та голосові повідомлення

Автором першого SMS-повідомлення став британець Ніл Папуорт.

За словами Ніла, на той момент йому було 22 роки, і він був розробником в компанії Vodafone. Перше в світі SMS-повідомлення з текстом "Щасливого Різдва" він відправив своєму начальнику 3 грудня 1992 року.

Примітно також, що повідомлення розробник відправив з комп'ютера, адже на той час мобільні телефони могли тільки приймати повідомлення.

Служба коротких повідомлень, смс-повідомлення, (англ. *SMS, Short Message Service*) — послуга обміну (передачі і прийому) короткими текстовими повідомленнями в телекомунікаційних мережах, доступна для більшості мобільних телефонів та інших комунікаційних пристроїв, таких як пейджер, модем, КПК, або навіть настільний комп'ютер (за допомогою функцій програмного забезпечення).

Для реалізації послуга повинна підтримуватись оператором зв'язку, комунікаційним пристроєм та програмним забезпеченням комунікаційного пристрою. Для випадку мобільного зв'язку для користування послугою потрібна SIM (USIM, R-UIM)-карта. Технологія смс-повідомлень підтримується мобільними мережами GSM, NMT, D-AMPS, CDMA, UMTS. Існує також послуга передачі текстових повідомлень на телефони стаціонарного (фіксованого зв'язку).

Максимальна стандартна довжина одного смс-повідомлення становить до 160 знаків латиницею або 70 кирилицею. Довші повідомлення розбиваються на кілька повідомлень.

В мережі Інтернет існує ряд сайтів, які надають можливість відправлення смс-повідомлень на мобільні телефони, зокрема сайти операторів мобільного зв'язку. Оператори зв'язку можуть обмежувати можливість прийому смс-повідомлень з інтернету, передачі смс-повідомлень на комерційні короткі номери та надавати абоненту можливість блокування таких повідомлень за допомогою сервісних (службових) смс-повідомлень або USSD-команд (запитів) (для запобігання спаму та шахрайства).

Послуга мультимедійних повідомлень (англ. *Multimedia Messaging Service*, MMS) — стандарт, який дозволяє пересилати між мобільними пристроями повідомлення з мультимедійним змістом (зображення, звук тощо), а не тільки з текстовим наповненням, як у випадку з SMS.

Голосова пошта (англ. *Voice-mail*) — це електронна система для реєстрації, збереження та перенаправлення телефонних голосових повідомлень (іноді - для розшуку та оповіщення користувачів).

В даний час під голосовою поштою розуміють два види сервісів, що надаються операторами і поштовими серверами:

- можливість для абонента телефонної мережі залишити адресату голосове повідомлення, яке той зможе прослухати пізніше.
- можливість прослухати по телефону збережені на сервері електронної пошти повідомлення, які читаються роботом.

Послугу голосової пошти надають абонентам практично всі оператори стільникового зв'язку і деякі оператори традиційної телефонії. Такий сервіс дозволяє записувати голосові повідомлення абонентів, доступ до яких потім можна отримати з телефону або через інтернет. Для користування послугою необхідний телефонний апарат, який може працювати в режимі частотного (тонового) набору номера.

У корпоративній телефонії під голосовою поштою (системою голосової пошти) розуміється пристрій, що підключається до офісної (службової) АТС на абонентські телефонні лінії і що дозволяє кожному абоненту АТС отримувати голосові повідомлення до персональної поштової скриньки.

Прослуховування повідомлень абонентом проводиться з телефонного апарату при дзвінку на певний телефонний номер.

Деякі системні телефонні апарати мають індикатор (лампочку), що інформує про появу нових повідомлень в поштовій скриньці.

Голосова пошта конструктивно може представляти собою:

- плату розширення офісної АТС (такі плати випускають виробники офісних АТС;
- самостійний пристрій для настільної установки (випускаються масою сторонніх виробників, використовується компаніями малого та середнього бізнесу);
- функціонально закінчений блок для установки в 19" стійку (також випускається сторонніми виробниками, використовується на великих і середніх підприємствах).

Сучасна голосова пошта оснащена автосекретарем, що забезпечує можливість донабору номера, а також можливість відправлення голосових повідомлень на e-mail-и абонентів (при підключенні до LAN).

9.8 Запитання до аудиторії

При розгляді однієї із цивільних справ про повернення боргу за договором позики, відповідачем по справі у якості доказу суду був наданий телефон із СМС повідомленням, яке ніби-то було направлено позивачем відповідачу і спростовувало певні обставини, на які посилався позивач у позовній заяві. Суд, прочитавши повідомлення, заслухавши пояснення позивача з даного приводу, який в свою чергу повідомив, що не надсилав це СМС-повідомлення вирішив, що такий доказ є неналежним і за власною ініціативою постановив ухвалу про направлення запиту в компанію-оператор мобільного зв'язку з метою отримання тексту та з'ясування, чи направлялося таке СМС повідомлення із одного номера на інший.

Чи має право оператор мобільного зв'язку на запит суду надавати таку інформацію?

Ст. 31 Конституції України кожному гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у

випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. Незважаючи на те, що в переліку кореспонденції прямо не зазначено СМС повідомлення, його все ж таки необхідно віднести до іншої кореспонденції оскільки воно має такі ж родові ознаки, як і листування, телефонні розмови, телеграфна кореспонденція: містить інформацію, яка для адресата або джерела надання інформації є таємницею і яку хоча б один із них не бажає довіряти іншим людям. Така позиція співпадає з підходами ЄСПЛ.

Що ж стосується можливості розкриття такої таємниці, то вона є правомірною тільки тоді, коли суд прийме рішення про необхідність розкриття такої інформації і тільки в тому випадку, якщо це допоможе запобігти злочину або з'ясувати істину під час розслідування кримінальної справи. *А це фактично означає, що по цивільній справі суд не мав права постановити ухвалу і направляти запит для отримання інформації, яка містилася у СМС повідомленні!(?)*

А якщо запит направлено, що тоді?

- Конституція України, безпосередньо ст. 31 та ст. 32.

Ч.2 ст. 32 Конституції України встановлює, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Тобто оператор мобільного зв'язку, маючи в своїй базі даних СМС повідомлення, крім підстав передбачених ст. 31 Конституції України, не має права розкривати його зміст, оскільки інформація, яка міститься в СМС повідомленні може бути конфіденційною.

- Відповідно до ст. 30 Закону України «Про інформацію» під конфіденційною інформацією розуміють відомості, які знаходяться у володінні користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Крім того ст. 37 Закону зазначає, що не підлягають наданню для ознайомлення за запитами документи та інформація, які містять у собі конфіденційну інформацію.

- В свою чергу, якщо існує заборона на вчинення певних дій, які вважаються протиправними, то повинна існувати і юридична відповідальність осіб, які вчинили такі дії. В нашому випадку необхідно звернути увагу на ст. 163 Кримінального кодексу України, який передбачає кримінальну відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Отже, право особи на таємницю кореспонденції ніби-то захищене і оператор мобільного зв'язку не повинен розкривати її на запит. Інакше працівники, винні у розголошенні таємниці кореспонденції, повинні бути притягнуті до кримінальної відповідальності.

Але існує ситуація при якій все ж таки право на таємницю кореспонденції більш за все буде проігноровано. Це може статися тоді, коли суд, на підставі ст. 84 Цивільного процесуального кодексу України, замість запиту направить до компанії-оператора ухвалу

про витребування тексту повідомлення, який може виступати доказом. От тоді ситуація явно може скластися не найкращим чином для автора СМС повідомлення.

9.9 Метадані

Метадані (у загальному випадку) — це дані, що характеризують або пояснюють інші дані. Наприклад, значення «123456» само по собі недостатньо виразно. А якщо значенню «123456» зіставлено достатньо виразне ім'я «поштовий індекс» (що вже є метаданими), то в цьому контексті значення «123456» більш осмислене — можна витягувати інформацію про місцезнаходження адресата, що має такий поштовий індекс. Оскільки для більшості людей різниця між словами «дані» та «інформація» є тільки з філософської точки зору і не істотна з практичної точки зору, то мають місце наступні визначення:

- Метадані – це інформація про дані.
- Метадані – це інформація про інформацію.

Інші визначення. Для терміну метадані немає єдиного формального визначення. Навпаки, існують різні визначення цього терміну. Ось ряд простих і популярних формулювань:

Метадані — це дані про дані. Цей термін в широкому сенсі слова використовується для будь-яких «даних про дані»: іменах таблиць, колонок в таблиці, програм і тому подібне.

Метадані — це дані з більш загальної формальної системи, що описує задану систему даних.

Метадані (Майкл Брекет) - будь-які дані про інформаційні ресурси організації.

Метадані (Адрієн Танненбаум) - детальний опис сутності даних.

Оскільки такі визначення мало що дають для розуміння суті метаданих, наведено їх основні характеристики:

- вони описують атрибути (характеристики) документа (інформаційного ресурсу);
- можуть автоматично генеруватись;
- дають потенційному користувачеві документа (інформаційного ресурсу) можливість отримати повну попередню інформацію про його існування та характеристики;
- «розуміються» комп'ютером (machine understandable).

Існують вужчі визначення:

Метадані — це структуровані дані, що являють собою характеристики описуваних сутностей для цілей їх ідентифікації, пошуку, оцінки, управління ними.

Метадані — це набір допустимих структурованих описів, які доступні в явному вигляді і призначення яких допомогти знайти об'єкт. Це визначення використовується набагато рідше, оскільки воно концентрується на одному з призначень метаданих — пошук об'єктів, сутностей, ресурсів — та ігнорує інші призначення.

Метадані - відомості, за допомогою яких описується структура, якість та інші характеристики просторових даних.

Структуровані у вигляді ієрархії метадані правильніше називати онтологією або схемою метаданих (наприклад, XML-схема).

Відмінність між даними та метаданими

Зазвичай, неможливо провести однозначне розділення на дані та метадані у документі, оскільки:

- Щось може бути як даними, так і метаданими. Так, заголовок статті можна одночасно віднести як до метаданих (як елемент метаданих — заголовок), так і до власне даних (оскільки заголовок є частиною самого тексту).
- Дані та метадані можуть мінятися ролями. На вірш, що розглядається як дані, може бути написана музика, в цьому випадку весь вірш може бути «прикріплений» до музичного файлу і в цьому випадку розглядається як метадані. Таким чином, віднесення до однієї або іншій категорії залежить від точки зору.

Можливе створення мета-мета-…-метаданих. Оскільки, відповідно до звичайного визначення, метадані є даними, то можна створити метадані на метадані, метадані на метадані на метадані і так далі. На перший погляд це може здатися безглуздим, але насправді це є дуже істотною і корисною властивістю даних і метаданих.

Ці міркування застосовні незалежно від вибору визначення метаданих (з приведених вище і не тільки).

Метадані можна класифікувати за таким ознаками:

Змістом. Метадані можуть або описувати сам ресурс (наприклад, назва і розмір файлу), або вміст ресурсу (наприклад, «у цьому відеофайлі показано як хлопець грає у футбол»).

Відношенням до ресурсу в цілому. Метадані можуть відноситься до ресурсу в цілому або до його частин. Наприклад, «Title» (назва фільму) відноситься до фільму в цілому, а «Scene description» (опис епізоду фільму) окреме для кожного епізоду фільму.

Можливістю логічного виводу. Метадані можна підрозділити на три шари: нижній шар — це «сирі» дані самі по собі; середній шар — метадані, що описують ці дані; і верхній шар — метадані, які дозволяють робити логічний вивід, використовуючи другий шар.

Різні дослідники виділяють різні класифікації метаданих. Одна з них включає в себе 3 групи:

Метадані, створювані web-службами індексування й пошуку (це дані, що збираються програмами-роботами на основі використання протоколу http і скриптів CGI для автоматичного створення записів на онлайнових інформаційних ресурсах).

Метадані, використовувані для опису інформаційного ресурсу (наприклад, формати Dublin Core та IAFA / WHOIS + + (проект ROADS); записи можуть створюватися вручну або автоматично).

Метадані, використовувані для завдання місцерозташування, аналізу, оцінки, документування і т.п. інформаційного ресурсу (такі метадані досить складні і дуже деталізовані, що вимагає залучення фахівців для їх розробки і супроводу).

Але більшість дослідників виділяє наступні типи метаданих:

описові, наприклад, бібліографічна інформація або інші відомості про зміст (семантику) цифрових об'єктів;

структурні, включаючи відомості про формати, структурі, об'ємі і інших формальних властивостях цифрових об'єктів;

адміністративні - права, дозволи на доступ, на корекцію даних, дані про користувача, дані для систем оплати, технологічні дані.

Особливим типом метаданих є ідентифікатор, завдання якого - однозначне уявлення цифрового об'єкта для зовнішнього світу і різних додатків.

Використання метаданих

Метадані використовуються для підвищення якості пошуку. Пошукові запити, використовуючи метадані, можуть врятувати користувача від зайвої ручної роботи з фільтрації. Інформуючи комп'ютер про те, які елементи даних зв'язані і як ці зв'язки враховувати, стає можливим здійснювати достатньо складні операції з фільтрації та пошуку.

Наприклад, якщо пошукова система «знає» про те, що «Ван Гог» є «голландським художником», то вона може видати у відповідь на запит про голландських художників веб-сторінку про Ван Гога, навіть якщо слова «голландський художник» не зустрічаються на цій сторінці. Такий підхід, званий представленням знань, знаходиться у сфері інтересів Семантичної павутини та штучного інтелекту.

Метадані стають важливі у World Wide Web внаслідок необхідності забезпечення пошуку корисної інформації серед величезної кількості доступної. Метадані, створені вручну, мають велику цінність, оскільки це гарантує свідомість. Якщо веб-сторінка на якусь певну тему містить слово або фразу, то всі інші веб-сторінки на цю тему можуть містити таке ж слово або фразу. Метадані також володіють різноманітністю, тому якщо з якоюсь темою зв'язано два значення, то кожне з них може бути використане. Наприклад, стаття про Живий Журнал може бути позначена за допомогою декількох значень: «Живий Журнал», «ЖЖ», «LiveJournal».

Зокрема, метадані створюються для оптимізації алгоритмів стиснення з втратою якості. Наприклад, якщо до відео додаються метадані, що дозволяють комп'ютеру розділити зображення на основну частину і фонову, то остання може бути стиснута сильніше, що дозволить досягти більшого коефіцієнта стиснення.

Деякі види метаданих призначені для забезпечення можливості різних видів представлення деяких даних. Наприклад, якщо до зображення додаються метадані, що містять інформацію про те, яка частина зображення найважливіша (припустимо, зображення людини), то програма для проглядання зображень на маленькому екрані (такому, як на мобільному телефоні), може відобразити тільки цю найважливішу частину зображення. Аналогічно використовуються метадані, що дозволяють зробити доступними для сліпих діаграми і зображення, шляхом їх перетворення для виведення на спеціальні

пристрої, або читання їх опису з використанням програмного забезпечення, що перетворює текст в мову.

Інші описові метадані можуть використовуватися автоматизованими робочими потоками. Наприклад, якщо деяка «розумна» програма «знає» вміст і структуру даних, то дані можуть бути автоматично перетворені і передані іншій «розумній» програмі як вхідні дані. В результаті, користувачі будуть врятовані від необхідності виконання безлічі рутинних операцій, якщо дані надані для роботи таким «небагатослівним» програмам.

Метадані використовуються для зберігання інформації про записи Audio CD. Аналогічно MP3 файли зберігають метадані у форматі ID3.

Практично кожний електронний документ має певні метадані. Метадані електронних документів відіграють важливу роль в системах електронного документообігу та автоматизації діловодства і інформаційно-пошукових системах. Метадані можуть, наприклад, включати дату, коли документ був збережений, і відомості про особистість користувача, що зберіг його. Системи електронного документообігу та автоматизації діловодства можуть також здобувати метадані з документу автоматично або підказувати користувачеві додати метадані.

9.10 Бази даних

Поняття «база даних»

Кожна людина у своєму житті часто зустрічаємося з необхідністю зберігання якої-небудь інформації . Наприклад, ми записуємо координатні дані потрібних осіб, номера телефонів своїх рідних та друзів, плануємо свій час тощо.

А куди вносимо цю інформацію? Правильно – у записну книжку. Саме вона, у нашому прикладі, є своєрідною базою даних. Для прикладу, той же довідник телефонних номерів являє собою таблицю. У ній розміщені такі дані, як номера телефонів, адреси їх власників і, власне, ініціали.

А уявіть собі, що таких схожих записів не два, як у прикладі, а три тисячі. І в одну мить працівник, що займається з таким довідником виявляє, що десь відбулася невідома помилка (друкарська помилка в самому номері телефону або в адресі проживання).

Напевне, буде не легко проводити процес пошуку недоліку, виявлення і виправлення помилки вручну. Такі страшні роздуми наводять на думку про необхідність засобів автоматизації процесів.

СКБД

Отже, для легкого і простого маніпулювання величезним обсягом даних програмісти і математики створили так звані системи керування базами даних або скорочено СКБД (іноді – СУБД). Якщо їх порівнювати із простими текстовими базами даних, то СКБД мають величезні переваги:

- ✓ можливість швидкого пошуку потрібної інформації
- ✓ взаємозв'язок усіх введених даних між собою

- ✓ використання даних різним програмних забезпеченням (наприклад, прикладними чи системними)
- ✓ одночасний доступ до інформації безлічі користувачів.

Виходить, база даних – це сукупність взаємозалежної інформації і даних, організованих і структурованих за певними правилами, що передбачають загальні принципи опису, зберігання і маніпулювання, незалежно від прикладних програм.

Звертання до баз даних, як уже було сказано, відбувається за допомогою систем керування базами, які забезпечують підтримку баз даних, керування і можливість доступу до бази користувачів.

10 ДОПУСТИМІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ

Мета навчання:

У цій главі ви дізнаєтесь, як усвідомлювати та зважати на деякі можливі пастки, здатні звести нанівець допустимість електронних доказів.

10.1 Підстави допустимості

Для Вас, як для суддів, оцінювання прийнятності доказів стане другою натурою, і Ви цілком звикнете до розгляду скарг на обґрунтованість і надійність доказів в інтересах справедливості та правосуддя.

Непостійний і швидкоплинний характер електронних доказів, мабуть, як ніколи раніше потребує від сторони обвинувачення підтверджень того, що вона дотримується всіх стандартів «гігієни», потрібних, щоби зберегти цілісність доказів. Як слід реагувати на випадки недотримання належної практики збору та опрацювання електронних доказів?

Наприклад:

Припустимо, що в системі зберігання речових доказів виявлено певні порушення: можливо, бракує деяких очевидних доказів, або не збігається час їхньої реєстрації.

Як би ви тоді стали розглядати такі сценарії?

Відповідальна посадова особа вибачається та пояснює, що, поки вони опечатували речові докази та оформлювали протокол їхнього вилучення, підозрюваний став агресивний, і його довелося вгамовувати. Ця особа мала на меті завершити оформлення після того, як ситуація стане спокійнішою, але забула внести до протоколу деякі подробиці.

Проти такого:

Жорсткий диск комп'ютера забрали зі сховища доказів на опрацювання й повернули за два дні, але в книзі обліку речових доказів немає жодних подробиць щодо того, що ж саме відбувалося з жорстким диском протягом цих двох днів. Відповідальна посадова особа каже, що вона нічого не пам'ятає, та, в будь-якому разі, не переймається занадто з приводу оформлення документів. Зрештою, важливими є результати аналізу, хіба не так?

В обох випадках точність чи обґрунтованість криміналістичного аналізу фактично можуть бути однакові, але порядок його виконання очевидно супроводжувався порушеннями. Сторона захисту може скористатися будь-якою невідповідністю, щоб оскаржити висновки експертизи, стверджуючи про неможливість довіряти доказам і наявність численних порушень. Утім, порушення можуть виникати під час проведення будь-яких процедур. Чи слід сповіщати сторону захисту про порушення процедури? Це питання, яке треба ставити до українського судочинства і судової практики.

10.2 Питання якості

У більшості випадків якість електронних доказів залежить від старанності та кваліфікації криміналіста, і там, де йому бракує знань, можуть виникати певні проблеми. Від фахівця, компетентного в одній конкретній сфері або в одному виді електронних доказів, не слід очікувати повноти знань з усього спектра цифрової криміналістики. Наприклад, фахівцям з аналізу пристроїв Windows може бракувати досвіду для того, щоб кваліфіковано

розбиратися з пристроями Apple або iPhone. Їхні операційні системи та файлові структури принципово відрізняються.

Те ж саме стосується й програмних засобів. Різні програмні засоби мають свої сильні та слабкі сторони, але неможливо гарантувати, що фахівець: (a) матиме доступ до останніх оновлених версій програм, найбільш придатних для виконання конкретного завдання; або (b) знатиме, як ними користуватися. Як ми вже висвітлювали вище, в справі Кейсі Ентоні,[53] таке поєднання може серйозно позначитися на якості аналізу та представлених у суді доказів.

Вище у цьому посібнику ми досить детально описували процес отримання образу оригінального диска, що становить речовий доказ. Як відомо, будь-яка дія над комп'ютером змінює стан пам'яті на цьому пристрої непередбачуваним чином.

Розглянемо ситуацію, коли серед видалених на комп'ютері обвинуваченого файлів вдалося відновити фрагмент такого змісту:

«… платіж у розмірі 45 000 дол. США мерові за сприяння угоді…»

Тепер припустимо, що слідчий з якихось причин здійснив пошук на цьому комп'ютері на місці злочину, але до того, як диск був вилучений. Неможливо дізнатися, чи внаслідок цього пошуку не були перезаписані дані, потрібні, щоб зрозуміти контекст цієї фрази. Сторона захисту може цілком впевнено стверджувати, що речення спочатку мало такий вигляд:

«Він вимагав платіж у розмірі 45 000 дол. США мерові за сприяння угоді, але я сказав йому, що повідомлю про нього поліції».

За браком інших підтверджувальних даних, це твердження сторони захисту неможливо буде спростувати.

А що казати про ситуацію, коли образ диску не був клонований через те, наприклад, що в криміналістичної лабораторії закінчився доступний дисковий простір? Це означатиме, що аналізи проводилися безпосередньо на вихідному диску.

У будь-якому разі, – чи то пошук непрофесійно здійснювався на місці злочину, чи то криміналістичний аналіз проводився на оригінальному диску, джерело доказів було забруднено. Якою мірою це впливає на прийнятність електронних доказів, – вирішувати вам.

Ми також обговорювали важливість хешування як способу забезпечення вірогідності криміналістичних копій. Чи допускаєте ви докази в тому разі, якщо хешування не застосовувалося або хеш-значення не збігаються?

Іншою простою, але важливою проблемою, здатною вплинути на вірогідність доказів, є мітки часу. Комп'ютер має внутрішній годинник, який може бути налаштований так, щоби показувати неправильний час, або може втратити точність із плином часу (це називається «відхиленням годинника»). Якщо внутрішній годинник на пристрої неточний, будь-які журнали чи записи подій на цьому пристрої матимуть неточну мітку часу. Ця різниця має братися до уваги, і потрібно зважати на таке розходження, особливо коли це стосується будь-яких журналів подій, створених іншими мережевими пристроями.

---

[53] http://www.4discovery.com/2012/11/29/casey-anthony-computer-forensics-investigators-overlook-google-search-for-fool-proof-suffocation-1/

Нам також відомо, що посилання на неточний час у зверненнях до постачальника послуг з вимогою надати відомості чи записи може спричинити проблеми через «динамічні» IP-адреси. Якщо точний час не зазначено, постачальнику чи партнеру за головною ліцензійною угодою можуть лише знадобитися додаткові уточнення, але якщо наведена в зверненні інформація неправильна, то цілком можливо, що у відповідь будуть надані неправильні дані.

Як вже обговорювалося, електронні докази по суті є непрямими, і треба доводити зв'язок між обвинуваченим і пристроєм на відповідний момент часу. Це особливо актуально, коли комп'ютером користуються декілька осіб.

Якщо комп'ютер перебуває у спільному користуванні, слід детальніше аналізувати поведінку користувачів. Наприклад, чи використовувалися логіни та паролі, щоб увійти в особисті облікові записи, які відомі лише підозрюваному та якими користується тільки він? Чи використовувався комп'ютер із цілями, специфічними для підозрюваного та пов'язаними з його інтересами? Чи здійснювалися в Інтернеті покупки з використанням платіжних карток підозрюваного?

Ще одним аргументом захисту, який успішно застосовувався в минулому, є твердження про те, що комп'ютер був начебто захоплений шкідливими програмами й що він насправді перетворився на «зомбі»-машину, якою дистанційно керував якийсь невідомий хакер без відома власника пристрою. Якщо криміналіст не спростує цей довід від самого початку, така аргументація здатна розвалити справу.[54]

Це лише декілька нюансів, що ілюструють потребу в грамотному та відповідальному поводженні з електронними доказами. Як і в усіх випадках, де розглядається допустимість доказів, саме Вам, суддям, доведеться вирішувати, якою мірою процедурні недоліки впливають на якість і надійність свідчень.

[54] Така аргументація з успіхом використовувалася у справах, що були пов'язані з дитячою порнографією, виявленою на комп'ютері обвинуваченого: https://www.nytimes.com/2003/08/11/business/acquitted-man-says-virus-put-pornography-on-computer.html, або див. https://www.cnet.com/news/a-child-porn-planting-virus-threat-or-bad-defense/

11 ТЕХНІЧНІ ТА ЮРИДИЧНІ ОСОБЛИВОСТІ КРИПТОВАЛЮТИ

11.1 Що таке криптовалюта?

Доволі часто можна почути, що криптовалюта не має жодної внутрішньої цінності. Це дійсно так і є, але ж і паперові гроші жодної власної цінності не мають, і навіть долар США не забезпечений золотом починаючи з 15 серпня 1971 року, тобто вже майже 50 років.[55] Нікого це не зупинило в його використанні. Можна навести ще один популярний аргумент скептиків – кожна держава забезпечує вартість своєї валюти, а вартість криптовалюти не забезпечує ніхто. Такий аргумент має певний сенс, але насправді вартість кожної валюти визначається ринком, тобто попитом та пропозицією, а держава лише вживає певні заходи регулювання в межах своєї компетенції.

У випадку криптовалюти її цінність та ліквідність забезпечується консенсусом певної кількості людей щодо її вартості. І якщо достатня кількість осіб вважає, що вартість однієї одиниці певної криптовалюти дорівнює, наприклад, 1 долару, і кожна з цих осіб готова цю криптовалюту обмінювати за таким курсом, то проблем із ліквідністю немає. Особливістю криптовалютного регулювання є децентралізація.[56] Це означає, що офіційного регулювання криптовалюти не існує.

Криптовалюта – вид цифрових грошей, які створені за допомогою криптографічних методів. Термін «криптовалюта» з'явився після появи системи Біткойн, яка була розроблена особою або групою осіб під псевдонімом Сатоши Накамото.[57] Зазвичай криптовалюти функціонують на основі технології блокчейн.

Станом на кінець листопада 2018 року існувало 2074 види криптовалюти.[58] Приблизно 25% з них не мають жодної вартості.

Криптовалюту також можна визначити як базу даних, яку не можна змінювати без дотримання визначених умов.

Криптовалютні одиниці зазвичай називають монетами (від англійської coin - монета). Але за своєю суттю це не монети, а хеш значення. Криптовалюти використовують технологію peer-to-peer, що означає пряму передачу даних між двома комп'ютерами, без будь-якої регуляції. Всі криптовалютні транзакції є незворотними. Єдине, що може змінити вже проведені транзакції – повернення блокчейну до стану на певний час у минулому, що може зробити тільки оператор блокчейну.[59]

Особливістю ринку криптовалют є неймовірна нестабільність курсу. Наприклад, капіталізація біткойну зменшилась втричі з грудня 2017 року по листопад 2018 року. Деякі криптовалюти взагалі зникають, втративши будь-яку вартість.

Ще однією проблемою криптовалюти є хакерські атаки. У разі злому криптовалютного гаманця, зловмисник отримує всі накопичені там монети. Також часто атакують

[55] https://www.forbes.com/sites/briandomitrovic/2011/08/14/august-15-1971-a-date-which-has-lived-in-infamy/#7639fb9a581a
[56]https://www.forbes.com/sites/dantedisparte/2018/06/19/when-it-comes-to-cryptocurrencies-to-the-sec-decentralization-is-key/#72bd037d796d
[57] https://www.quora.com/Who-is-most-likely-Satoshi-Nakamoto-the-inventor-of-Bitcoin
[58] https://coinmarketcap.com/all/views/all/
[59] https://bitcoin.stackexchange.com/questions/197/can-a-bitcoin-transaction-be-reversed

криптовалютні біржі. Наприклад, Японія втратила більше ніж 540 мільйонів доларів за перше півріччя 2018 року внаслідок хакерських атак. Слід звернути увагу, що з цих 540 мільйонів, 518 було викрадено з криптобірж, а 22 – з приватних гаманців.[60]

11.2 Блокчейн

Блокчейн – це побудований за певними правилами безперервний ланцюг блоків, які містять інформацію. Кожен блок складається із заголовку та списку транзакцій і обов'язково містить хеш попереднього блоку. Таким чином, блокчейн містить дані про всі транзакції з самого початку роботи, і копії цієї бази даних зберігаються одночасно на багатьох ПК. Інформація в блоках є відкритою, а відсутність змін підтверджується за допомогою криптографічних методів. Необхідно підкреслити, що внаслідок збереження даних про всі транзакції, база даних блокчейн зберігає і може показати всю історію власності щодо кожної монети.

Безперервність та незмінність системи забезпечується включенням до кожного блоку хеш значення попереднього блоку, що не дозволяє змінити інформацію в певному блоці без зміни хеш значень в наступних блоках. Залежно від конкретної криптовалюти, блок формується внаслідок виконання певної роботи (proof of work), наявності певної суми на рахунку (proof of stake) або внаслідок надання певних ресурсів (proof of space).

В Україні також запроваджується використання технології блокчейн. Наприклад, Міністерство аграрної політики та продовольства України спільно з Державним агентством електронного урядування та Transparency International Україна презентували оновлений Державний земельний кадастр, який відтепер працюватиме на технології Blockchain. Упровадження цієї технології дозволить забезпечити надійну синхронізацію даних, що унеможливить їх підміну в результаті зовнішнього втручання, а також дасть можливість здійснювати суспільний контроль за системою. Запровадження технології блокчейн затверджено постановою КМУ № 688 від 21.06.2017 року.[61]

Згідно з даними інституту дослідження блокчейну, Україна входить до 14 світових лідерів з блокчейну.[62]

11.3 Зарубіжне регулювання криптовалют

Правовий режим регулювання криптовалют, зокрема біткойна, відрізняється залежно від держави. В Німеччині біткойн визнано платіжним засобом.[63] В Японії криптовалюти також є платіжним засобом, за їх допомогою можна навіть оплачувати комунальні послуги.[64]

Ситуація щодо регулювання обігу криптовалюти динамічно змінюється у всьому світі.

22 жовтня 2015 року Європейський Суд Справедливості постановив, що операції обміну криптовалют на фіатні (паперові) гроші звільняються від ПДВ. При цьому в США криптовалюти відносять до категорії товарів.

---

[60] https://www.coindesk.com/japan-lost-540-million-to-crypto-hacks-in-first-half-of-2018
[61] http://zakon.rada.gov.ua/laws/show/688-2017-%D0%BF
[62] https://www.ukrinform.net/rubric-economy/2390351-ukraine-listed-among-leaders-in-blockchain-innovation.html
[63] https://strana.ua/news/127517-v-hermanii-ofitsialno-priznali-platezhnym-sredstvom-kriptovaljutu-bitkoin.html
[64] https://blog.ipleaders.in/cryptocurrency-japan-approach/

Наразі все більше держав вживають заходи, спрямовані на чітке законодавче визначення криптовалют, а також на створення певних механізмів регулювання. Колишня директор Міжнародного Валютного Фонду Крістін Лагард зазначала, що запровадження державного регулювання криптовалют є неминучим, і це є тільки питанням часу.[65]

11.4 Національне законодавство щодо регулювання криптовалют

Згідно з роз'ясненням НБУ від 10.11.2014 року Національний банк України розглядає "віртуальну валюту/криптовалюту" Bitcoin як грошовий сурогат, який не має забезпечення реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це протирічить нормам українського законодавства.[66]

Згідно зі спільною заявою фінансових регуляторів від 30.11.2017 року Національний банк України, Національна комісія з цінних паперів та фондового ринку і Національна комісія, що здійснює регулювання у сфері ринків фінансових послуг, переконані, що складна правова природа криптовалют не дозволяє визнати їх ані грошовими коштами, ані валютою і платіжним засобом іншої країни, ані валютною цінністю, ані електронними грошима, ані цінними паперами, ані грошовим сурогатом.[67]

Таким чином позиція НБУ значно змінилась з 2014 року. У Верховній Раді України свого часу було зареєстровано законопроект № 7183 від 06.10.2017 року про обіг криптовалюти в Україні. Законопроект пропонував таке визначення криптовалюти – програмний код (набір символів, цифр та букв), що є об'єктом права власності, який може виступати засобом міни, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду).[68]

Усталеної судової практики з приводу використання криптовалют поки не існує. Певний інтерес становить постанова Харківського окружного адміністративного суду від 13 жовтня 2016 року у справі № 820/5120/16, в якій позивач оспорив податкові консультації ГУ ДФС у Харківській області щодо оподаткування ПДВ операцій з криптовалютами.

Рішенням Дарницького районного суду м. Києва від 24.03.2016 року у справі № 753/599/16-ц відмовлено у позові про зобов'язання передати біткойни в якості товару в натурі. Суд мотивував це рішення тим, що не може зобов'язати відповідача передати позивачу речі, які не мають ознак матеріального світу. Ухвалою Апеляційного суду міста Києва від 12.10.2016 року вказане рішення залишено без змін.

Слід відмітити, що у наведеній постанові адміністративного суду помилково наведено посилання на Європейський Суд Справедливості як на Європейський суд з прав людини (справа «Хедквіст проти Швеції»).

Що стосується кримінальних проваджень, є відносно усталена практика надання дозволів на обшук та арешт майна, такого як обладнання для виробництва (майнінгу) криптовалют. Зазвичай підозра пред'являється за статтями 190, 200 та 209 КК України. При цьому,

[65] https://www.bbc.com/ukrainian/news-43031351
[66] https://www.bank.gov.ua/control/uk/publish/article?art_id=11879608
[67] https://bank.gov.ua/control/uk/publish/article?art_id=59735329&cat_id=55838
[68] http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

жодного вироку тільки за статтею 200 КК України немає, а за статтею 209 КК України (відмивання коштів) із використанням криптовалюти наявні 5 вироків; в усіх затверджено угоду про визнання винуватості, і всі вони стосуються відмивання коштів від продажу наркотичних засобів на території РФ.

Що стосується відкритого використання криптовалюти в Україні, слід згадати про відкриття першого біткойн-банкомату в Одесі 03.05.2017 року.[69] На теперішній час таких банкоматів в Україні десятки, і навіть деякі пункти обміну валют пропонують послуги з обміну криптовалюти.[70]

11.5 Використання криптовалюти у відмиванні коштів або іншого майна, одержаних внаслідок вчинення суспільно небезпечного протиправного діяння

Необхідно відмітити, що криптовалюта використовується, в тому числі, для відмивання грошей.

Керівник Департаменту кіберполіції Національної поліції України Сергій Демедюк 29.01.2018 року повідомив, що де-факто, за всіма ознаками криптовалюта може відноситься до електронних коштів - одиниць вартості, які зберігаються на електронному пристрої і приймаються як засіб платежу. У той же час, контроль за її трансакціями забезпечується криптографічним захистом.

Відтак, незважаючи на те, що по своїй сутності існування й обіг криптовалюти базується на основах фінансової піраміди, кіберполіція підтримує ідею легалізації криптовалюти в Україні, а також процесу її майнінгу (щонайменше, це прирівняти її до електронних коштів). Також підтримується ідея використання технології Blockchain у державному та приватному секторах.

Сергій Демедюк також додав, що усі операції з криптовалютою в Україні мають бути з обов'язковою ідентифікацією власника криптовалютного гаманця, так як основною проблемою правоохоронців у світі є саме підтвердження права власника гаманця на його власність.[71]

Роб Уейнрайт, керівник Європолу, 12.02.2018 року зазначив, що 3-4 мільярда фунтів брудних грошей щорічно відмиваються в Європі за допомогою криптовалют. Анонімна та нерегульована природа криптовалют приваблює злочинців, та ускладнює поліції їх відстеження, оскільки складно ідентифікувати, хто саме здійснює перекази. А у випадках встановлення кримінальної сутності переказів немає можливості заморозити активи, на відміну від звичайної банківської системи.[72]

Міжнародна група з протидії відмиванню брудних грошей (ФАТФ) (англ. Financial Action Task Force on Money Laundering), визначає відмивання грошей як процес перетворення злочинних доходів з метою приховати їх справжнє джерело. Такий процес є дуже

[69] https://cryptocurrency.tech/v-odesse-poyavilsya-pervyj-bitkoin-bankomat/
[70] https://www.google.com.ua/maps/search/bitcoin/@50.4209201,30.4785814,12z
[71] http://old.npu.gov.ua/mvs/control/main/uk/publish/article/2226198;jsessionid=C27F7C9C6983A8D91CC6C690B8D9BFE6
[72] https://www.bbc.com/news/technology-43025787

важливим, оскільки дозволяє злочинцю розпоряджатись прибутком, не ставлячи під загрозу джерело доходу.[73]

Тобто суть відмивання грошей полягає в тому, що гроші, природу яких особа не може пояснити, стають легально отриманими і відкритими. У випадку простого переведення брудних грошей у криптовалюту, з'являється брудна криптовалюта, і особа так само не може пояснити, звідки вона. Після проведення зворотної операції знову з'являються брудні гроші. Тобто просте переведення одного виду активу в інший без застосування традиційних методів відмивання грошей нічого не дає.

Але стаття 209 КК України визначає відмивання грошей (Легалізація (відмивання) доходів, одержаних злочинним шляхом – назва статті) іншим чином: вчинення фінансової операції чи правочину з коштами або іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів, а також вчинення дій, спрямованих на приховання чи маскування незаконного походження таких коштів або іншого майна чи володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення, зміну їх форми (перетворення), а так само набуття, володіння або використання коштів чи іншого майна, одержаних внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів.

Отже, згідно з законодавством України для наявності складу злочину, передбаченого ст. 209 КК України, достатньо здійснення будь-якої операції з коштами чи іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння; достатньо навіть володіння.

Певна популярність криптовалюти серед злочинців обумовлена її децентралізацією та легкістю проведення транскордонних операцій. Головною проблемою при розслідуванні таких злочинів є ідентифікація власника криптовалютного гаманця.

Як ми зазначали раніше, в Україні є вироки за ст. 209 КК України за фактами, пов'язаними із використанням криптовалюти. Так, у справі № 754/1786/18 обвинувачений отримав злочинний дохід в РФ від продажу наркотичних засобів, а потім в Україні обмінював електронні гроші з Ківі гаманця на біткойни за допомогою інших осіб.

Незважаючи на популярність криптовалюти серед злочинців, загальна тенденція її використання значно змінилась за останні роки. І якщо раніше 90% операцій з криптовалютами були асоційовані з кримінальними діями, то на теперішній час – навпаки.[74]

При цьому, як зазначає Ліліта Інфанте з Управління по боротьбі з наркотиками США, блокчейн насправді надає нам багато інструментів для того, щоб ідентифікувати людей. І вона висловлює побажання, щоб люди продовжили використовувати криптовалюти.[75]

Її позиція є зрозумілою, оскільки насправді криптовалюти не є абсолютно анонімними, а є псевдоанонімними. Дійсно, блокчейн не має даних щодо власника гаманця, тобто його

[73] http://www.fatf-gafi.org/faq/moneylaundering/
[74] https://forklog.com/upravlenie-po-borbe-s-narkotikami-ssha-vsego-10-bitkoin-tranzaktsij-svyazany-s-kriminalom/
[75] https://www.ccn.com/dea-criminal-activities-account-for-just-10-percent-of-bitcoin-transactions/

ПІБ, адресу тощо. Але кожна транзакція є відкритою в мережі, кожен може побачити розмір, час та номери гаманців. І, як і в інших випадках використання інтернету, можна відстежити IP-адресу користувача.

Згідно з дослідженнями Університету Люксембургу, навіть у випадку використання браузера TOR, атака типу «особа посередині» є ефективним засобом злому, і може розкрити реальну IP-адресу та надати всю інформацію щодо здійснюваних транзакцій, навіть у разі використання засобів захисту.[76]

[76] https://www.coindesk.com/bitcoin-tor-anonymity-can-busted-2500-month

12 МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПРИ ЗБОРІ ЕЛЕКТРОННИХ ДОКАЗІВ

Мета навчання:

Надання учасникам інформації щодо способів отримання електронних доказів від країн із іншими правовими системами (інших юрисдикцій).

Зміст

За допомогою практичних прикладів будуть висвітлені такі питання:

- Національне регулювання міжнародної допомоги
- Юридичні та практичні аспекти направлення запитів про міжнародну правову допомогу
- Різниця між відкритими та закритими даними
- Можливості та обов'язки за Будапештською конвенцією
- Отримання від основних постачальників комерційних послуг даних без розголошення інформаційного вмісту повідомлення (non-content data)

12.1 Національне регулювання міжнародної допомоги

Ефективний захист порушених, оспорюваних чи невизнаних прав, свобод та інтересів в умовах сьогодення є неможливим без адекватної правової регламентації статусу та порядку застосування електронних доказів. Нормативне регулювання інституту доказування у процесуальних кодексах на національному рівні не є досить чітким у частині використання інформаційно-телекомунікаційних технологій. З огляду на це відповіді на питання про порядок залучення електронних доказів у процес слід шукати у наднаціональних актах, які регулюють особливості транскордонного судочинства.

В ієрархії норм права за юридичною силою одразу за конституційно-правовими слідують норми міжнародно-правових актів. За ч. 1 ст. 9 Конституції України чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Частина 4 ст. 9 Кримінального процесуального кодексу України встановлює примат норм міжнародно-правових актів над нормами національного законодавства: «У разі якщо норми цього Кодексу суперечать міжнародному договору, згода на обов’язковість якого надана Верховною Радою України, застосовуються положення відповідного міжнародного договору». Аналогічні положення містяться і в решті процесуальних кодексів України.

З наведеного випливає, що якщо процесуальне законодавство України не регулює питання, пов’язані з електронними доказами, їх можна вирішувати, керуючись положеннями чинних міжнародних договорів України. Проте серед міжнародних договорів України немає таких, які б встановлювали певні стандарти доказування в кримінальних, цивільних чи адміністративних справах. Відтак, норми міжнародно-правових актів у судах України застосовуються лише у тих випадках, коли у справі наявний так званий іноземний елемент.

Слід констатувати, що чинні міжнародні договори України, норми яких регулюють питання процесу доказування у судочинстві з іноземним елементом, не містять положень про електронні докази. Зокрема, цілий ряд конвенцій, які стосуються цивільного процесу (Конвенція з питань цивільного процесу 1954 року, Конвенція про отримання за кордоном доказів у цивільних або комерційних справах 1970 року, Конвенція про вручення за кордоном судових та позасудових документів у цивільних або комерційних справах 1965 року, Європейська конвенція про інформацію щодо іноземного законодавства 1968 року, Угода про порядок вирішення спорів, пов'язаних із здійсненням господарської діяльності 1992 року), Конвенція про правову допомогу і правові відносини у цивільних, сімейних і кримінальних справах 1993 року - не містять жодних положень, які б регулювали будь-які аспекти застосування електронних доказів у міжнародному цивільному процесі.

Єдиним міжнародним договором України, що безпосередньо торкається питань, пов'язаних із електронними доказами, є Конвенція про кіберзлочинність 2001 року, статті якої визначають повноваження договірних держав на збирання доказів у електронній формі стосовно кримінальних правопорушень.

Причин для такого «відставання» вбачається декілька. По-перше, більшість міжнародних договорів з питань судочинства, згода на обов'язковість яких надана Верховною Радою України, були укладені іще у XX столітті, коли інформаційно-телекомунікаційні технології не мали такого поширення як сьогодні, тому вони залишили питання електронних доказів осторонь з цілком об'єктивних причин. По-друге, на сьогодні регулювання процесуальних відносин щодо використання електронно-інформаційних систем збереження та передачі інформації здійснюється у кожній країні по-різному. Тому уніфікація норм національного законодавства є пріоритетним завданням для наддержавних утворень та організацій, але, водночас, доволі складним і довготривалим. По-третє, через відсутність уніфікації процесуальних норм на міждержавному рівні високим є ризик виникнення правозастосовних непорозумінь між державами під час надання правової допомоги у справах. Зокрема, проблеми можуть з'явитися внаслідок різних законодавчих підходів до визнання електронних доказів належними, допустимими чи достовірними (приклад: посвідчення копій електронних доказів нотаріусами в Російській Федерації та в Україні).

Проте становище України не є абсолютно катастрофічним, оскільки міжнародно-правові норми деяких із вищезазначених актів забезпечують непряму можливість використання електронних доказів у судочинстві з іноземним елементом. Міжнародні договори України можуть бути як багатосторонніми, так і двосторонніми. Звідси процесуально-правові норми, що можуть регулювати питання застосування електронних доказів, слід шукати не лише у багатосторонніх конвенціях, а й у двосторонніх договорах. На сьогодні Україна є учасником цілого ряду чинних двосторонніх договорів про правову допомогу та правові відносини у кримінальних справах.

Для того, щоб запит про міжнародну правову допомогу мав юридичну силу, необхідно, щоб у запитуваній юрисдикції ці дії також визнавалися правопорушенням з такими ж або схожими злочинними діями.

12.2 Конвенція про правову допомогу та правові відносини у цивільних, сімейних і кримінальних справах 1993 року

У рамках СНД було ратифіковано Конвенцію про правову допомогу та правові відносини у цивільних, сімейних і кримінальних справах 1993 року, стаття 6 якої зобов'язує договірні сторони надавати одна одній правову допомогу шляхом виконання процесуальних та інших дій, передбачених законодавством запитуваної сторони, зокрема складання і пересилання документів, вилучення, пересилання і видачу речових доказів, проведення експертизи, допиту сторін, свідків, експертів, визнання і виконання судових рішень у цивільних справах. Таке формулювання нормативного положення дещо звужує можливості транскордонного обміну електронними доказами, проте не забороняє, зокрема: 1) складання та пересилання електронних документів; 2) вилучення, пересилання та видачу, як речових доказів, магнітних, електронних та інших носіїв інформації, що містять аудіовізуальну інформацію про обставини, що мають значення для цивільної справи; 3) складання та пересилання протоколів огляду електронних доказів; 4) допиту експертів чи спеціалістів з питань, що можуть стосуватися використання електронних доказів в інтересах судочинства в Україні; 5) проведення експертизи електронно-обчислювальних машин чи електронних інформаційних систем.

При застосуванні Конвенції рекомендуємо ознайомитись із роз'ясненням ГУЮ у Дніпропетровській області «Практичні аспекти застосування судами України Конвенції про правову допомогу та правові відносини у цивільних, сімейних і кримінальних справах 1993 року», де наведені зразки оформлення доручень та детально роз'яснено правила направлення запитів про міжнародну правову допомогу.

12.3 Міжнародні угоди про надання правової допомоги

На нашу думку, найбільш ефективними та універсальними для практичного використання є Європейська конвенція про взаємну допомогу у кримінальних справах 1959 року (дата підписання 20.04.1959 року, дата підписання Україною 29.05.1997, дата ратифікації 16.01.1998, дата набуття чинності 09.06.1998), Конвенція про кіберзлочинність 2001 року (Будапештська Конвенція) (дата підписання 23.11.2001, дата ратифікації 07.09.2005, набула чинності 01.07.2006 року) та Конвенція про правову допомогу та правові відносини у цивільних, сімейних і кримінальних справах 1993 року (Мінська Конвенція) (дата підписання 22.01.1993 року, ратифікована 10.11.1994 року, набула чинності 14.04.1995 року).

Також у цьому контексті необхідно згадати Кримінальну конвенцію про боротьбу з корупцією 1999 року (дата підписання 27.01.1999, дата ратифікації Україною 18.10.2006, дата набрання чинності для України 01.03.2010).

При виборі конвенції чи міжнародного договору, якими буде найбільш доцільно скористатись, необхідно перш за все перевірити, які саме міжнародні договори укладені між Україною та державою, до якої буде направлено запит.

Для витребування електронних доказів найбільш доцільним вбачається застосування Будапештської Конвенції про кіберзлочинність. На дату написання цього посібника Конвенцію ратифікувала 61 держава, і це єдина конвенція, яка стосується саме електронних доказів та кримінальних правопорушень, пов'язаних із комп'ютерними технологіями.

Аналіз досвіду сторін Європейської конвенції Ради Європи про кіберзлочинність (який також стосується обміну електронними доказами щодо інших кримінальних правопорушень) показав, що відповідно до вимог конвенції, опрацювання запитів триває від 6 місяців до 2 років (а іноді і значно довше).[77] Такі результати характерні для спільноти країн, які юридично, дипломатично та політично зобов'язані обмінюватися такими даними. Не можна недооцінювати вплив політичного аспекту. Ворожнеча між державами (або, принаймні, підозра та недовіра), також, відіграє роль, зокрема у мотивації до обробки запитів про міжнародну правову допомогу (MLA) або відповіді на них.

Триває чимало суперечок щодо того, коли (і навіть якщо) дані знаходяться в кіберпросторі, то яку юрисдикцію у такому випадку слід застосовувати. Ті, хто підтримує традиційну, найпоширенішу думку, вважають, що дані перебувають в юрисдикції тієї країни, де розміщено сервер з даними. Отже, закони, які врегульовують роботу з даними, стосуються й розміщення сервера.

Але як бути у ситуації, коли слідчий хоче скористатися доказами з газети, чи надрукувати інформацію з google-карт чи зі сторінки Facebook? Строго кажучи, чи повинні ці докази бути прийнятними за відсутності запиту про MLA? Чи необхідно це погоджувати з владою країни, де розміщено сервер?

Необхідно розмежовувати відкриті та закриті дані. Відкриті дані – це такі дані, до яких можна отримати вільний доступ та ознайомитися з їхньою суттю. Відповідно до Принципу 6 (a) «Принципів транскордонного доступу до збережених комп'ютерних даних» 1999 року з групи країн Великої вісімки,[78] офіційний дозвіл на доступ до «публічно доступних (з відкритим вихідним кодом) даних» не вимагається «незалежно від того, де дані географічно розташовані».

Можливо, більш цікавим є формулювання Принципу 6 (b). Дозвіл від країни, де здійснюється пошук, також, не потрібен для: «Доступу, пошуку, копіювання чи вилучення даних, що зберігаються в комп'ютерній системі, яка розташована в іншій державі в разі вчинення дій з урахуванням законної або добровільної згоди особи, яка має законне право розкривати ці дані».

Ці принципи містять аналогічні положення Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція). У статті 23 зазначено:

«Сторони співробітничають між собою у найширших обсягах відповідно до принципів цього розділу шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Аналогічні положення містяться і в статті 25 Конвенції:

---

[77] Доступ кримінального правосуддя до даних у хмарі: Співпраця з «іноземними» постачальниками послуг http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

[78] https://www.justice.gov/sites/default/files/ag/legacy/2004/06/09/99TransborderAccessPrinciples.pdf

«Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення».

Особливий інтерес становить стаття 32 Будапештської конвенції:

«Будь-яка Сторона може, не отримуючи дозвіл іншої Сторони:

a. здійснювати доступ до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або

b. здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи».

Звичайно, якщо Будапештська Конвенція не ратифікована державою, куди необхідно направити запит, необхідно шукати інші способи.

Наприклад, у разі направлення запиту до Російської Федерації або Республіки Беларусь, які не ратифікували Будапештську Конвенцію, можна скористатись Мінською Конвенцією.

12.4 Регулювання міжнародної допомоги у КПК України

Слід звернути увагу, що згідно зі ст. 545 КПК України, під час досудового розслідування із запитами про міжнародну правову допомогу звертається Генеральна прокуратура України, а під час судового провадження – Міністерство юстиції України.

З наведеного можна зробити висновок, що у разі звернення слідчого чи прокурора до слідчого судді з таким клопотанням, в його задоволенні слід відмовляти, а у разі прийняття рішення про направлення запиту про міжнародну правову допомогу на стадії судового розгляду слід звертатись до Міністерства юстиції України в порядку та у формі, що визначені відповідним міжнародним договором та статтею 552 КПК України.

Що стосується виконання запитів про міжнародну правову допомогу Україною, є достатньо усталена практика, і зазвичай такі запити задовольняються.

Так, ухвалою слідчого судді Малиновського районного суду м. Одеси від 30.01.2018 року у справі № 1-м/521/19/18 задоволено клопотання слідчого по матеріалам запиту Французької Республіки та надано доступ до інформації про власника кожної IP-адреси, всіх технічних даних і звітності, пов'язаних з підпискою на інтернет-послуги (особа абонента, дата початку контракту, засоби платежу), інформації про характеристики ліній (фіксований або динамічний IP), у випадках динамічного IP, до договорів оренди, пов'язаних з підпискою з моменту її створення, типу сервера (виділений, загальний...), умов, пов'язаних з його використанням (тип договору), а також характеру пов'язаних з ним послуг (веб-сервер, PTP, електронна пошта...), технічних даних, пов'язаних з управлінням і адмініструванням сервера, включаючи IP-адреси підключення на консоль адміністрування, інформації чи

підписався власник сервера на інші договори: іншу лінію / сервер, ім'я домену, по IP адресам[79]

Згідно зі ст. 552 КПК України, запит повинен містити: 1) назву органу, який звертається за допомогою, та компетентного органу запитуваної сторони; 2) посилання на відповідний міжнародний договір або на дотримання засади взаємності; 3) найменування кримінального провадження, щодо якого запитується міжнародна правова допомога; 4) стислий опис кримінального правопорушення, що є предметом кримінального провадження, та його правову кваліфікацію; 5) відомості про повідомлену підозру, обвинувачення з викладенням повного тексту відповідних статей Кримінального кодексу України; 6) відомості про відповідну особу, зокрема її ім'я та прізвище, процесуальний статус, місце проживання або перебування, громадянство, інші відомості, які можуть сприяти виконанню запиту, а також зв'язок цієї особи із предметом кримінального провадження; 7) чіткий перелік запитуваних процесуальних дій та обґрунтування їхнього зв'язку із предметом кримінального провадження; 8) відомості про осіб, присутність яких вважається необхідною під час виконання процесуальних дій, і обґрунтування цієї необхідності; 9) інші відомості, які можуть сприяти виконанню запиту або передбачені міжнародним договором чи вимогою компетентного органу запитуваної сторони.

У разі відсутності міжнародного договору з певною державою, залишається спосіб, передбачений статтею 544 КПК України, згідно з якою за відсутності міжнародного договору України міжнародна правова допомога чи інше співробітництво може бути надано на підставі запиту іншої держави чи запитано на засадах взаємності. Уповноважений (центральний) орган України, направляючи до такої держави запит, письмово гарантує запитуваній стороні розглянути в майбутньому її запит про надання такого самого виду міжнародної правової допомоги.

За відсутності міжнародного договору з відповідною державою уповноважений (центральний) орган України надсилає запит про надання міжнародної правової допомоги до Міністерства закордонних справ України для подальшого передання його компетентному органу запитуваної сторони дипломатичним шляхом.

Порядок оформлення таких запитів детально не регламентований, і, на нашу думку, в цьому випадку слід керуватись загальними правилами направлення запитів, що встановлені ст. 552 КПК України, тобто детально мотивувати необхідність запитуваної інформації для встановлення істини у справі, наводити посилання на докази наявності обґрунтованої підозри особи у вчиненні злочину, яка виправдовує втручання у права особи (у разі направлення запиту, що порушує такі права), зазначати всі необхідні відомості, які потрібні для виконання запиту.

12.5 Докази постачальника послуг у США

Оскільки всі основні постачальники послуг (за винятком тих, що розташовані в Азії) базуються в США, був ризик того, що Міністерство юстиції США «завалять» запитами на отримання електронних даних. Тому воно прийняло рішення дозволити правоохоронним органам надсилати прямі запити до постачальників послуг США, але лише щодо даних

[79] http://reyestr.court.gov.ua/Review/71870258

про трафік/транзакції (якщо в запиті вимагається вміст будь-яких електронних доказів, то вимога щодо надсилання офіційного запиту про MLA залишається в силі).

Прямий запит на отримання даних повинен чітко містити правову основу, на якій він базується, і його має спрямовувати «затверджений» національний орган. На відміну від обов'язку щодо надання відповіді у статті 32 (2) Будапештської конвенції, постачальник послуг не зобов'язаний надавати відповідь або, навіть, підтверджувати отримання запиту. Це цілком дискреційний процес.

Як ви можете собі уявити, оскільки це є дискреційною процедурою за участю приватного бізнесу, вимоги та політика значно відрізняються в кожній компанії та можуть змінюватися. Однак загальним елементом є можливість вимагати надання термінових відповідей у надзвичайних ситуаціях. Прикладом надзвичайних умов стали терористичні напади на журнал Charlie Hebdo у Парижі в 2015 році. За вимогою французького правоохоронного органу було отримано інформацію про обліковий запис електронної пошти терориста упродовж 45 хвилин.

Порада щодо таких прямих запитів була зазначена в одному документі колишнім королівським прокурором Великої Британії Деном Сатером (Dan Suter). Його «Інструкція з отримання доказів від американських постачальників послуг зв'язку» була підготовлена у 2015 році, тому вона трохи застаріла. Наразі готується нова інструкція, яку, як очікується, буде опубліковано Управлінням ООН з наркотиків і злочинності.[80]

Наведені нижче посилання містять вказівки щодо того, як зробити запит до кількох відомих постачальників послуг. Ця інформація була актуальною влітку 2017 року, але, можливо, що вона зазнала змін.

Apple:

www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

www.apple.com/legal/privacy/law-enforcement-guidelines-emeia.pdf

www.apple.com/legal/privacy/law-enforcement-guidelines-apac.pdf

DropBox 2015:

www.dropbox.com/transparency

Facebook:

www.facebook.com/safety/groups/law/guidelines

Google:

www.google.com/transparencyreport/userdatarequests/legalprocess/

---

[80] Тим часом копію випуску 2015 року можна знайти за цим посиланням: www.irisinvestigations.com/wordpress/wp-content/uploads/2016/12/Toolbox/12-SUBPOENA%20GUIDE-SAMPLES/Communication%20Service%20Providers%20Guidance%202015.pdf

Instagram:

help.instagram.com/494561080557017/

Linkedin:

help.linkedin.com/app/answers/detail/a_id/16880/~/linkedin-law-forforcement-data-request-guidelines

Microsoft:

www.microsoft.com/about/csr/transparencyhub/pppfaq/

www.microsoft.com/about/csr/transparencyhub/lerr/

Pinterest:

help.pinterest.com/en/articles/law-enforcement-guidelines

Snapchat:

www.snap.com/en-GB/privacy/transparency/

Tumblr:

www.tumblr.com/docs/law_enforcement

Twitter:

support.twitter.com/articles/41949-guidelines-for-law-enforcement#

Yahoo:

transparency.yahoo.com/law-enforcement-guidelines/us

Цей режим добровільного розкриття інформації не є досконалим. Аналіз 189 289 запитів щодо абонентських даних в 2014 році (знову за участю Сторін Будапештської конвенції) показав, що лише на 68% таких запитів надано відповідь, що містять дані від постачальників послуг. Постачальники послуг повідомили такі причини, чому запити часто залишаються без відповіді:

- Дані відсутні
- запит неналежно сформовано
- надано неточні дані
- неможливо перевірити дійсність юридичних повноважень щодо підготовки такого запиту.

12.6 Нова ініціатива ЄС

Навесні 2018 року ЄС надав пропозицію щодо нового Європейського порядку представлення доказів. Цей порядок має полегшити доступ до електронних доказів між країнами-членами ЄС за допомогою загального шаблону, і запровадить норму для підготовки відповіді на строк до 10 днів у стандартних випадках та протягом 6 годин у

надзвичайних ситуаціях.[81] Станом на початок 2019 року робота із запуском порядку була практично завершена.

Подальшу інформацію про пропозицію до Регламенту Європейського Парламенту та Ради про європейський порядок представлення та зберігання електронних доказів у кримінальних справах можна знайти за цим посиланням:

https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

Копію додатків із запропонованим шаблоном запиту можна знайти за цим посиланням:

https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_2&format=PDF

[81] http://europa.eu/rapid/press-release_MEMO-18-3345_uk.htm

13 Електронна пошта

Мета навчання:

На цьому занятті ви дізнаєтеся про приховану інформацію, що міститься в звичайному електронному листі.

Ми вже коротко вели мову про те, що називається заголовком електронного листа, і побачили, що в ньому містяться відомості про трафік, які показують, коли і як електронну пошту доставляють до вашої поштової скриньки. На цьому занятті ми трохи глибше поринемо в заголовки електронної пошти та дослідимо інформацію, яку вони містять.

Як ми вже бачили, всі електронні листи мають електронний заголовок, однак способи доступу до них залежать від постачальника послуг. Ось короткий огляд того, як можна відкрити заголовок електронного листа на веб-сайтах деяких популярних сервісів електронної пошти (станом на початок 2019 року)

Gmail:	«Показати оригінал» у розкривному меню зверху праворуч від повідомлення електронної пошти
Hotmail Outlook mail	«Показати джерело повідомлення» у розкривному меню зверху праворуч від повідомлення електронної пошти

Інформація в заголовку дуже компактна й може виявитися досить складною для аналізу, але в рамках цього курсу достатньо зрозуміти основні принципи, знаючи типи даних, які можна відновити, і що вони можуть містити.

Якщо на секунду замислитися над тим, як надсилаються звичайні листи, це допомогло б зрозуміти концепцію заголовка електронного листа та процес, що він уособлює.

Коли Ви хочете надіслати листа, Ви кладете його в конверт, пишете на ньому адресу призначення (а іноді й зворотну адресу) та йдете з ним до поштового відділення, де на нього наклеюють поштову марку, а працівник поштової служби його штемпелює. Таким чином, якщо тоді подивитися на конверт, то можна побачити, хто надіслав листа, куди він прямує та країну походження (з поштової марки). Про дату відправлення та місце, де лист потрапив до поштової служби, можна дізнатися зі штемпеля.

Від приймального поштового відділення лист передадуть до сортувального центру (де, можливо, на нього поставлять ще один штемпель), після чого він на своєму шляху пройде ще через один або декілька сортувальних центрів. У кожному центрі читатимуть адресу призначення, і листа передаватимуть до наступного центру по ланцюжку, доки він не дістанеться найближчого до призначення сортувального центру. Після цього він потрапить до сумки листоноші, який віднесе його за адресою та опустить до поштової скриньки.

Якщо уявити собі поштове відділення та сортувальні центри як сервери електронної пошти в Інтернеті, кожен з яких читає та додає свою інформацію на конверті, то можна буде зрозуміти, що таке заголовок електронного листа. Вивчення зовнішньої сторони конверта може багато чого повідати про шляхи передавання та походження листа.

Заголовок електронного листа, використаний у наведеному нижче прикладі, взято з реального фішингового електронного листа, що був надісланий на адресу поштового

сервісу Google. Як можна побачити з позначки у верхньому лівому куті зображення, система помітила, що це «фішингове» повідомлення, і автоматично перемістила його до теки «Спам».

У цьому повідомленні є низка текстових підказок, які вказують на те, що все в ньому не так, як мало би бути:

- численні лексичні та граматичні помилки;
- воно нікому конкретно не адресоване (тобто надіслано невідомій кількості одержувачів прихованих копій);
- ім'я відправника не збігається з адресою електронної пошти (яка, як видається, є загальною службовою груповою адресою електронної пошти, що належить університету в Аргентині);
- у тексті йдеться про неймовірно щедру пропозицію повному незнайомцю;
- одержувачу пропонується натиснути на посилання в тілі повідомлення.

На тлі інших фішингових електронних листів це не дуже складне чи переконливе повідомлення, але розглянемо заголовок електронного листа та подивимося, чи ми можемо ще щось знайти.

Повний заголовок листа виглядає так:

```
Delivered-To: destinatiionX@gmail.com
Received: by 2002:XXX:3fc2:0:0:0:0:0 with SMTP id w2-v6csp2190685qth;
        Sun, 27 May 2018 22:50:50 -0700 (PDT)
X-Google-Smtp-Source: ADUXVKIoDGEfsuvpJLH3dRrSSkkqNw6IHKMF3cH0yaHsUPJTbp1QIEWvQXNFGttWfhs0MTdINV+W
X-Received: by 2002:XXX:4589:: with SMTP id l9-v6mr11238609qtn.255.1527486650341;
        Sun, 27 May 2018 22:50:50 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1527486650; cv=none;
        d=google.com; s=arc-20160816;
        b=u+LjQQ4bcOV9FjYnU5UkpeXf2kWIssV7/IDy4GFYEbZsktzVzBTrM5DT90r99cuZcB
         UM0uKyokwSTfPTU6WYelSg1olzvcUa0HRqj1T7aYVdo1004J3ue6P1c8CKmxtzQKukxK
         /+puw849HcGJQRqCCxAaePTCvGR7jfDIvY28mOT55vGDh6qylu/6hwjomfEOjcyLI8G+
         EwbmGVFmN/zHChHI9JuCgTqEJnwOLVdHj+hNCTJu9UhAGurqonvkNU9uPsP3q0W0IW7s
         SSqZ06nrUSnRm+poJ5Kjhj03hT4v7aXnZkS8XCMn+yHSJJ0puHoTokVITuLjXU8mPILw
         xRtA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=reply-to:date:from:to:subject:content-description
         :content-transfer-encoding:mime-version:message-id
         :arc-authentication-results;
        bh=J63HGrbWRTveAf9z554J0TLxSEatdtvR8rJnKqYQm/Q=;
        b=By9JyktmoI6DEogPtasCBfd7Su5HadXnB4eGC8x0za/D0Ns5di1I987oKpXNXQsXHx
         g+UDAwzF1WheZ7J7Tb+jGwb3Zwfq/ils6B8yKde4xuluHCW4Dj7TXSAUYvqvxmnYybmp
         xTsekctrcVemA9mGid7LRO+OVE0mfAaD8HPsepQZrGJZVMRMEyZSGbDC7vYNE0k+SSeA
         s9smLJcoLRT2bAW4yzak2wSHihPCMas4vPF6WJinMa9SAGlaUfq5cXVKKEPk9BgaH/VX
         5n8cSFb9uEJlGOpgk18ypjhJGg6l26Q5vtYZP9HszRYdgFoTweSz+o7OfQOfUvL4kVuy
         qByw==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of info@fceia[redacted].edu.ar designates 200.3.XXX.XXX as permitted sender)
smtp.mailfrom=info@fceia[redacted].edu.ar
Return-Path: <info@fceia[redacted]r.edu.ar>
Received: from mailgw.fceia[redacted]r.edu.ar (mailgw.fceia[redacted].edu.ar. [200.3.XXX.XXX])
        by mx.google.com with ESMTPS id y10-v6si3247045qkl.355.2018.05.27.22.50.48
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sun, 27 May 2018 22:50:50 -0700 (PDT)
Received-SPF: pass (google.com: domain of info@fceia[redacted]r.edu.ar designates 200.3.XXX.XXX as permitted sender) client-ip= 200.3.XXX.XXX;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of info@fceia[redacted].edu.ar designates 200.3.XXX.XXX as permitted sender)
smtp.mailfrom=info@fceia[redacted].edu.ar
Received: from eva.fceia[redacted]r.edu.ar (eva-new.n.fceia[redacted]r.edu.ar [10.66.50.197] (may be forged)) by mailgw.fceia[redacted].edu.ar
(8.14.4/8.14.4/Debian-8+deb8u2) with ESMTP id w4S5nOZ7032012; Mon, 28 May 2018 02:49:40 -0300
Received: from [172.20.10.2] ([105.112.96.209]) (authenticated bits=0) by eva.fceia[redacted]r.edu.ar (8.14.4/8.14.4/Debian-8+deb8u2) with
ESMTP id w4RJiJLH017398 (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT); Mon, 28 May 2018 02:46:52 -0300
Message-Id: <201805280546.w4RJiJLH017398@eva.fceia[redacted].edu.ar>
Content-Type: text/plain; charset="iso-8859-1"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Description: Mail message body
Subject: Re: Grant-
To: Recipients <info@fceia[redacted]r.edu.ar>
From: "M. M. Fridman" <info@fceia[redacted]r.edu.ar>
Date: Mon, 28 May 2018 08:37:35 +0300
Reply-To: mikh.fridman@gmail.com
X-Scanned-By: Sistema de filtrado de FCEIA on 200.3.123.187
X-Virus-Scanned: clamav-milter 0.99.4 at eva.fceia[redacted]r.edu.ar
X-Virus-Status: Clean

I Mikhail Fridman. has selected you specially as one of my beneficiaries
for my Charitable Donation, Just as I have declared on May 23, 2016 to give
my fortune as charity.

Check the link below for confirmation:

http://www.ibtimes.co.uk/russias-second-wealthiest-man-mikhail-fridman-plan=
s-leaving-14-2bn-fortune-charity-1561604

Reply as soon as possible with further directives.

Best Regards,
Mikhail Fridman.
```

Звертаємо увагу на те, що основні елементи адрес електронної пошти та IP-адрес в заголовку були змінені або замасковані, щоб захистити непричетних до цього осіб, а адресу електронної пошти було змінено на destinationX@gmail.com.

Заголовок електронного листа аналізується чи «читається» знизу вгору, оскільки нові дані додаються зверху заголовка на кожному черговому етапі його передання (тобто щоразу, коли він проходить через «сортувальний» сервер). Інакше кажучи, верхня частина заголовка повідомлення показує останні додані дані.

Заголовок повідомлення читають знизу вгору.

Розглянемо окремі розділи заголовка.

У першому розділі (внизу) показано метадані повідомлення:

```
Message-Id: <201805280546.w4RJiJLH017398@eva.fceia.u edu.ar>
Content-Type: text/plain; charset="iso-8859-1"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Description: Mail message body
Subject: Re: Grant-
To: Recipients <info@fceia. edu.ar>
From: "M. M. Fridman" <info@fceia. .edu.ar>
Date: Mon, 28 May 2018 08:37:35 +0300
Reply-To: mikh.fridman@gmail.com
X-Scanned-By: Sistema de filtrado de FCEIA on 200.3.XXX.XXX
X-Virus-Scanned: clamav-milter 0.99.4 at eva.fceia. edu.ar
X-Virus-Status: Clean
```

Як ви вже знаєте, «метадані» – це дані, які описують чи щось говорять про інші дані. Метадані в заголовку електронного листа містять огляд основних інформативних заголовків.

«Message–Id» (ідентифікатор повідомлення) – це унікальне посилання, за яким можна ідентифікувати цього конкретного електронного листа. У цьому прикладі (в інших системах може бути інакше) «Message–Id» починається з адреси та часу повідомлення, що вказує на час його оброблення сервером. Далі йде контрольне число, а потім, після значка @, – назва сервера (eva.fceia.XXX.edu.ar). Хоча повну назву сервера приховано, вона належить до того ж університету в Аргентині. На жаль, зловмисники можуть налаштувати комп'ютер як сервер і назвати його як завгодно, зокрема зімітувати назву справжнього сервера.

«Content-Type» (тип контенту) описує формат, в якому був складений текст повідомлення.

«MIME-Version» посилається на версію багатоцільового розширення пошти в Інтернеті (Multipurpose Internet Mail Extensions), що використовувалася для відправлення

повідомлення. Протокол MIME дозволяє вставляти в електронний лист зображення, аудіо та відеозаписи, а також текст, символи якого не входять до кодування ASCII.[82]

Далі можна побачити адресу електронної пошти, на яку було надіслано повідомлення («To:», тобто «кому»), а також адресу з якої його було надіслано («From:», тобто «від кого»). Ми вже звернули увагу на те, що адреси електронної пошти як відправника, так і одержувача в цих метаданих однакові (що вказує на використання прихованих копій) і що обліковий запис відправника начебто вказує на відправлення від імені фізичної особи, але обліковий запис електронної пошти очевидно належить до групової службової адреси електронної пошти. Однак, слід також зазначити, що адреса «Reply-To:» (зворотна) перенаправляє всі відповіді на безкоштовну облікову адресу Gmail (що виглядає як вельми дивний вибір з боку «другої за статками в Росії людини» для використання з метою благодійних пожертвувань).

Як ми вже бачили, обліковий запис електронної пошти відправника та назва сервера вказують на те, що повідомлення надійшло з аргентинського університету. Примітка іспанською (X-Scanned-By: Sistema de filtrado de FCEIA on 200.3.XXX.XXX) начебто підтверджує зв'язок з Аргентиною.

Однак у часі відправлення очевидні деякі невідповідності. Метадані вказують на те, що листа було відправлено в понеділок, 28 травня, о 08:37:35 +0300 (тобто UTC[83] плюс три години), однак Message-Id показує час 05:46 (тобто тригодинна різниця в часі, що свідчить про часовий пояс UTC). Утім, для Аргентини часовий пояс становить UTC мінус три години; отже логічно припустити, що час мав бути 02:46.

```
Received: from eva.fceia.    edu.ar (eva-new.n.fceia.    edu.ar
[10.66.XXX.XXX] (may be forged)) by mailgw.fceia.    .edu.ar
(8.14.4/8.14.4/Debian-8+deb8u2) with ESMTP id w4S5nOZ7032012;
Mon, 28 May 2018 02:49:40 -0300
Received: from [172.20.10.2] ([105.112.96.209]) (authenticated
bits=0) by eva.fceia.    edu.ar (8.14.4/8.14.4/Debian-8+deb8u2) with
ESMTP id w4RJiJLH017398 (version=TLSv1/SSLv3 cipher=DHE-RSA-
AES256-SHA bits=256 verify=NOT); Mon, 28 May 2018 02:46:52 -0300
```

На цьому рисунку ми бачимо перші два «мережні сегменти» або кроки, через які пройшов лист. Кожен мережний сегмент починається з позначки: Received: from

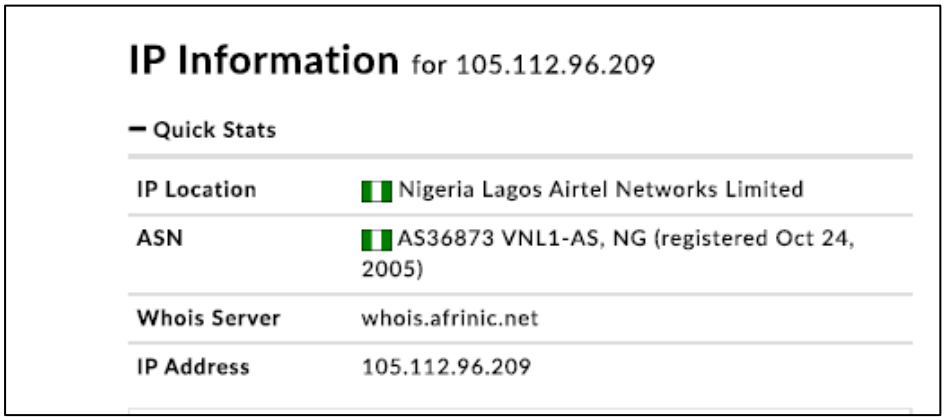
Якщо порівняти мітку часу на першому мережному сегменті – нижньому з двох записів – з моментом відправлення повідомлення, то вона дійсно показує 02:46:52.

Подивимось також на показані IP-адреси. Перша зареєстрована IP-адреса (172.20.10.2) належить до групи IP-адрес, що можуть існувати лише всередині приватної мережі (тобто зарезервовані для використання системними адміністраторами та в закритих мережах). Друга IP-адреса, як видається, вказує на фактичне походження цього листа, але якщо ми

[82] Про ASCII ми дізналися на першому занятті.

[83] UTC – це абревіатура Coordinated Universal Time (всесвітній координований час), що відповідає часу за гринвічським меридіаном плюс одна секунда.

перевіримо цю другу IP-адресу (105.112.96.209) за допомогою пошукового сервісу Whois, то виявиться, що вона належить Інтернет-провайдеру в Нігерії, а не розташована в Аргентині.



IP Information for 105.112.96.209

— Quick Stats

IP Location	Nigeria Lagos Airtel Networks Limited
ASN	AS36873 VNL1-AS, NG (registered Oct 24, 2005)
Whois Server	whois.afrinic.net
IP Address	105.112.96.209

Система помічає щось підозріле під час оброблення, оскільки другий сервер у ланцюжку (котрий також входить до університетської мережі та має внутрішню IP-адресу 10.66.XXX.XXX) помічає заголовок попередженням «можливо підроблений» (may be forged).

```
spf=pass (google.com: domain of info@fceia.   edu.ar designates
200.3.XXX.XXX as permitted sender) smtp.mailfrom=info@fceia.   edu.ar
Return-Path: <info@fceia.   edu.ar>
Received: from mailgw.fceia.   .edu.ar (mailgw.fceia.   .edu.ar.
[200.3.XXX.XXX])
      by mx.google.com with ESMTPS id y10-
v6si3247045qkl.355.2018.05.27.22.50.48
      (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256
bits=128/128);
      Sun, 27 May 2018 22:50:50 -0700 (PDT)
Received-SPF: pass (google.com: domain of info@fceia.   .edu.ar
designates 200.3.XXX.XXX as permitted sender) client-ip=200.3.XXX.XXX;
Authentication-Results: mx.google.com;
     spf=pass (google.com: domain of info@fceia.   edu.ar designates
200.3.XXX.XXX as permitted sender) smtp.mailfrom=info@fceia.   .edu.ar
```

На цьому подальшому етапі ми бачимо, що повідомлення нарешті отримане на google.com та зареєстроване на сервері google mx (mail exchange – обмін поштовими повідомленнями) після надходження з поштового сервера аргентинського університету (mailwk.fceia.XXX.edu.ar, який має зовнішню IP-адресу 200.3.XXX.XXX).

«SPF» означає Sender Policy Framework (структуру політики фільтрації відправників) і є механізмом перевірки назви облікового запису відправника за переліком затверджених облікових записів електронної пошти, яким дозволяється надсилати повідомлення з певного домену. У цьому випадку ви можете побачити, що повідомлення пройшло

перевірку SPF, оскільки в ньому зазначено: «domain of info@fceia.XXX.edu.ar designates 200.3.XXX.XXX as permitted sender» (домен info@fceia.XXX.edu.ar призначає 200.3.XXX.XXX дозволеним відправником).

Зверніть увагу, що показаний час змінився на -0700 UTC або на тихоокеанський літній час, тобто на пояс, де у Google є принаймні один центр оброблення даних. Різниця в часі також означає, що дата змінилася з понеділка 28 травня на неділю 27 травня.

```
ARC-Seal: i=1; a=rsa-sha256; t=1527486650; cv=none;
      d=google.com; s=arc-20160816;
      b=u+LjQQ4bcOV9FjYnU5UkpeXf2kWIssV7/IDy4GFYEbZsktzVzBTrM5DT90r99cuZcB
       UM0uKyokwSTfPTU6WYeISg1olzvcUa0HRqj1T7aYVdo1004J3ue6P1c8CKmxtzQKukxK
       /+puw849HcGJQRqCCxAaePTCvGR7jfDIvY28mOT55vGDh6qylu/6hwjomfEOjcyLl8G+
       EwbmGVFmN/zHChHI9JuCgTqEJnwOLVdHj+hNCTJu9UhAGurqonvkNU9uPsP3q0W0lW7s
       SSqZ06nrUSnRm+poJ5Kjhj03hT4v7aXnZkS8XCMn+yHSJJ0puHoTokVITuLjXU8mPlLw
       xRtA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
      h=reply-to:date:from:to:subject:content-description
       :content-transfer-encoding:mime-version:message-id
       :arc-authentication-results;
      bh=J63HGrbWRTveAf9z554J0TLxSEatdtvR8rJnKqYQm/Q=;
      b=By9Jyktmol6DEogPtasCBfd7Su5HadXnB4eGC8x0za/D0Ns5di1l987oKpXNXQsXHx
       g+UDAwzF1WheZ7J7Tb+jGwb3Zwfq/ils6B8yKde4xuIuHCW4Dj7TXSAUYvqvxmnYybmp
       xTsekctrcVemA9mGid7LRO+OVE0mfAaD8HPsepQZrGJZVMRMEyZSGbDC7vYNE0k+SSeA
       s9smLJcoLRT2bAW4yzak2wSHihPCMas4vPF6WJinMa9SAGlaUfq5cXVKKEPk9BgaH/VX
       5n8cSFb9uEJlGOpgk18ypjhJGg6I26Q5vtYZP9HszRYdgFoTweSz+o7OfQOfUvL4kVuy
       qByw==
ARC-Authentication-Results: i=1; mx.google.com;
```

ARC (Authenticated Received Chain – ланцюжок автентифікованого отримання повідомлень) становить ще одну форму перевірки автентичності, яка є досить нова й ще не широко розповсюджена. Цей механізм здійснює перевірку автентичності повідомлень, що проходять через проміжні сервери, порівнюючи цифровий підпис кожного повідомлення з тим, що був створений на початку відправлення повідомлення. ARC призначений виявляти спроби внесення змін до повідомлень, що передаються між серверами. Тут вартим уваги є лише використання алгоритму SHA256[84] для генерування цифрового підпису.

[84] Алгоритм криптографічного шифрування SHA ми розглядали раніше у цьому посібнику.

```
Delivered-To: destinationX@gmail.com

Received: by 2002:XXX:3fc2:0:0:0:0:0 with SMTP
id w2-v6csp2190685qth;
      Sun, 27 May 2018 22:50:50 -0700 (PDT)
X-Google-Smtp-Source:
ADUXVKIoDGEfsuvpJLH3dRrSSkkqNw6IHKMF3cH0yaHsUPJTbp1QlEWv
QXNFGttWfhs0MTdlNV+W
X-Received: by 2002:XXX:4589:: with SMTP
id l9-v6mr11238609qtn.255.1527486650341;
      Sun, 27 May 2018 22:50:50 -0700 (PDT)
```

У цій останній частині заголовка електронного листа ми бачимо, що повідомлення нарешті було доставлено на цільовий сервер для одержувача «destinationX@gmail.com». Оскільки адреса – це обліковий запис Google, повідомлення залишається на сервері, доки його не перегляне користувач.

Онлайнові інструменти можуть полегшити аналіз заголовків повідомлень. Наприклад, якщо відкрити веб-сторінку за наведеним нижче посиланням, то можна самостійно проаналізувати заголовок електронного листа:

https://mxtoolbox.com/EmailHeaders.aspx

Проте такі інструменти зазвичай здатні лише на поверхневий аналіз.

Важливо також пам'ятати, що зловмисники не можуть змінити ті дані в заголовку електронного повідомлення, котрі містяться у верхньому (тобто останньому) записі. Все інше може підроблюватися. До того ж, оскільки облікові записи електронної пошти можна легко створювати, надаючи неправдиві дані, результатом цього може бути виникнення фальшивих слідів. З іншого боку, заголовки електронних повідомлень, надісланих компаніями або приватними постачальниками послуг електронної пошти, можуть дійсно виявитися вельми корисними. У всякому разі, їх не можна ігнорувати під час розслідування, і вони потребують перевірки.

У цьому розділі ми розглянули деякі подробиці, які можна знайти в заголовку одного лише повідомлення електронної пошти, але, як ми вже переконалися раніше, корисною інформацією про власника облікового запису також може володіти постачальник послуг електронної пошти з метою ефективного управління та адміністрування облікового запису користувача.

На сьогодні постачальники комерційних послуг часто пропонують користатися єдиним логіном для всіх своїх продуктів. Наприклад, Microsoft пропонує єдиний логін для Microsoft Store, користування Office 360, а також для поштових послуг Hotmail/Outlook, тоді як Google надає доступ до Google Play і YouTube за тими ж обліковими даними, що потрібні для входу на пошту Google. Це цілком може означати, що у постачальника послуг є дані не лише про ім'я власника облікового запису, а також, можливо, про інші форми

ідентифікації або навіть номер кредитної картки та адреса для виставлення рахунків за користування іншими послугами чи продуктами.

Коли хтось відкриває декілька облікових записів електронної пошти на різні імена, їх часто підтверджують за тим же номером телефону чи додатковою адресою у разі, якщо пароль буде втрачений. Такі подробиці також можуть допомогти у встановленні особи користувача.

Ще одним потенційно корисним джерелом інформації є архів IP-адрес, що використовувалися під час доступу до електронної пошти. Ми знаємо, як можна використати IP-адреси, щоби встановити місцезнаходження підозрюваного, але ми також знаємо, як легко їх можна замаскувати чи скористатися загальною точкою доступу WiFi. Однак там, де можна встановити закономірність серед IP-адрес, це здатне забезпечувати такий рівень передбачуваності, на який можна покладатися в оперативних цілях.

MAC-адреси (якщо вони відомі) також можуть виявитися корисними в ідентифікації реального пристрою, що використовувався для надсилання електронного листа в мережі.

Насамкінець, записи про транзакції на обліковому записі електронної пошти (тобто надіслані та отримані електронні повідомлення), навіть за відсутності даних про зміст цих повідомлень, можуть містити подробиці про співучасників або іншу інформацію про суб'єкта, яка потім може бути використана з метою визначення особистісних характеристик підозрюваного.

Контрольні запитання:

1. Чому заголовок повідомлення читають знизу вгору?

Вивчення та повторення:

Відкрийте заголовок повідомлення, що надійшло вам електронною поштою. Спробуйте визначити основні елементи заголовка, зокрема IP-адресу, з якої надійшло повідомлення, і часову шкалу, а також різні сервери, через які йшло повідомлення.

14 Висновки

Ця збірка навчачльних матералів тренінгу підготовлена в рамках навчального курсу «Застосування електронних доказів під час розгляду справ, пов'язаних з корупцією». Тепер Ви краще розумієте, де шукати електронні докази, як їх застосовувати та оцінювати, можете професійно допитувати експерта, ставлячи йому питання не тільки юридичної спрямованості, а й технічної. В опрацьованих Вами матеріалах також показано, як приховують та спотворюють електронні докази, і за якими критеріями можна оцінити їх допустимість. Ви також дізнались, як законодавчо регулюється питання застосування електронних доказів, та які міжнародні договори можна використовувати при міжнародному співробітництві.

15 ДОДАТКИ

15.1 Практичні вправи

Додаток 1. Практична вправа щодо використання даних геопозиції та координат базових станцій

ПРИМІРНИК УЧАСНИКА

Полковник Недовірятенко П. обвинувачується в отриманні неправомірної вигоди при закупівлі військового обладнання. Обвинувальний акт передано до суду. Прокурор вказує, що Недовірятенко П. отримував неправомірну вигоду від Fullen Defense LLC– виробника військового обладнання в США. Неправомірна вигода була надана Джеррі Кожошуа, громадянином США, який покинув Україну. Розслідування щодо нього було виділене в окреме провадження і зараз триває.

Прокурор стверджує, що Недовірятенко та Кожошуа неодноразово зустрічались в Парку Вічної Слави, зокрема в період з 1 травня 2018 року по 31 серпня 2018 року. На цих зустрічах обговорювались деталі корупційних махінацій та передачі неправомірної вигоди. Факт зустрічей підтверджено даними радіорозвідки та порівнянням геолокаційних даних з телефонів Недовірятенка та Кожошуа.

Особистий номер телефона П. Недовірятенка - 0192838475 (IMEI 23 856253 398494 2) з 1 травня 2018 року по 31 серпня 2018 року. Телекомунікаційний провайдер – CallmeUa.

Джеррі Кожошуа має зареєстрований в Україні номер 0574838291 (IMEI 35 780502 763722 2). Телекомунікаційний провайдер пана Джеррі Кожошуа – ApaFone.

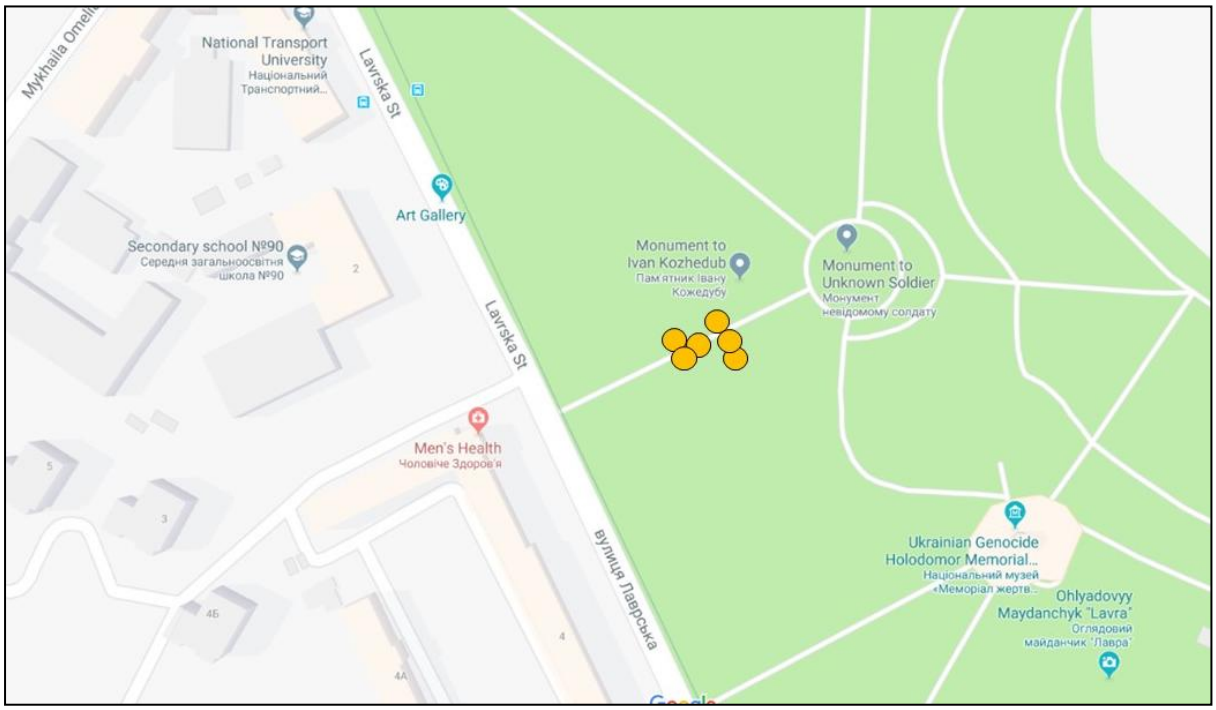
Телефон полковника Петра Недовірятенка – це смартфон iPhone, але GPS був вимкнений, тому доступна лише геолокація з вузлу стільникової мережі. У Києві CallmeUa використовує 500 вузлів стільникового зв'язку (базових станцій). У складі вузлу стільникового зв'язку міститься антена, яка забезпечує точку з'єднання для здійснення дзвінків. Антенний комплекс CallmeUa складається з трьох (3) панелей, кожна з яких покриває певний сектор під кутом 120 градусів (забезпечуючи тим самим повне 360° покриття). Коли телефон входить до сектору дії антени, він автоматично реєструє свою присутність на цій антені та генерує реєстраційний запис. У місті, де є більша кількість таких споруд стільникового зв'язку як антени та вежі, одна антена, зазвичай, покриває площу від 1,3 до 5 кв.км, але це залежить як від щільності мережі базових станцій, так і від рельєфу місцевості. У сільській місцевості, де антен менше, кожен такий сектор може охоплювати територію площею до 200 кв.км. Однак, можна значно точніше визначити місцезнаходження телефону за допомогою аналізу стільникового зв'язку, який полягає в перевірці того, як, коли та де сигнал телефону з'єднується з базовими станціями, а також де сигнали сходяться. Часто це потребує відвідування місця для того, щоб відмітити на мапі телефонні сигнали.

У смартфоні пана Джері Коджошуа активовано функцію GPS. GPS – це глобальна система позиціонування, і її робота залежить від супутникової технології. Смартфон підключається до GPS-сигналу кожні декілька секунд до тих пір поки включений телефон. Незважаючи на те, що місцевість та будівлі можуть впливати на якість GPS-сигналу, зазвичай, вважають, що він може визначити локацію людини в межах 5-8 м.

У відповідні дати записи даних GPS зі смартфону пана Джеррі Коджошуа свідчать про те, що він перебував у Парку Вічної Слави кожного разу в різний час з 13:10 до 13:55:

2018	GPS-координати	Початок часового відліку	Кінець часового відліку
28 червня	50.438845, 30.552486	13:12:06	13:33:20
26 червня	50.438808, 30.552630	13:14:31	13:41:10
12 червня	50.438862, 30.552341	13:10:18	13:32:47
22 травня	50.438842, 30.552406	13:15:02	13:39:18
8 травня	50.438842, 30.552251	13:12:47	13:55:01

Ці GPS-координати визначають місце розташування Парку Вічної Слави, як показано на цій карті.

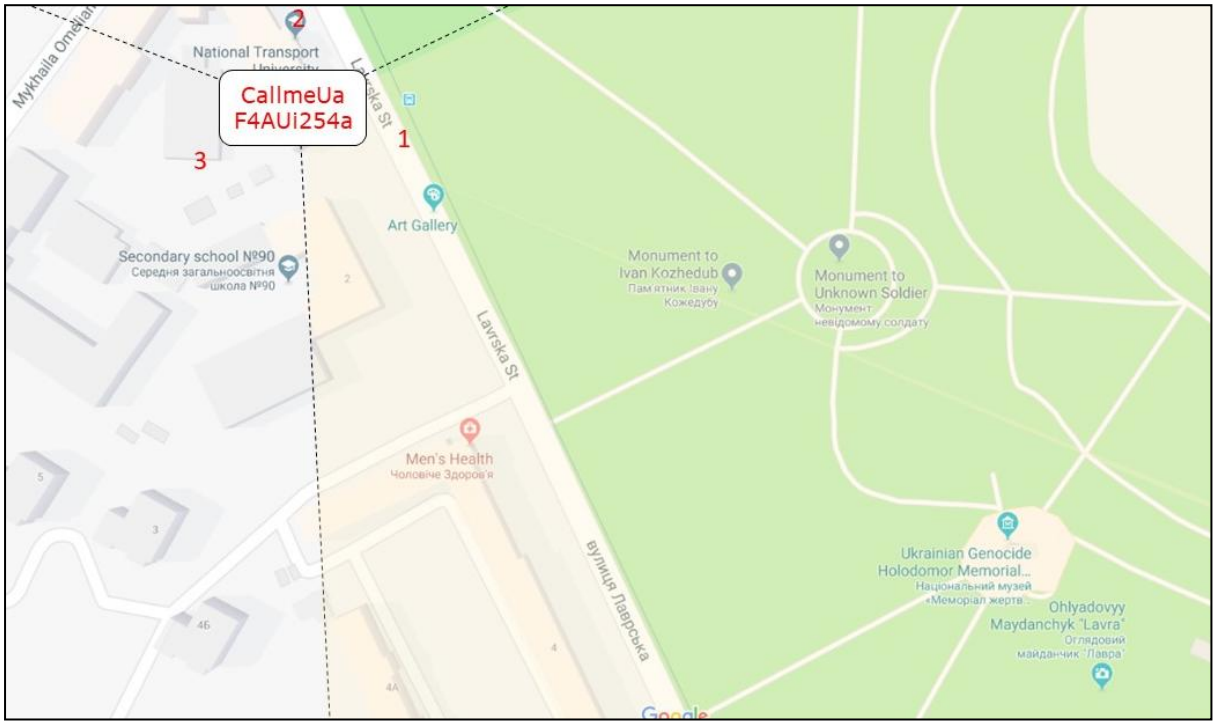


Телефон полковника П. Недовірятенка був зареєстрований в антенному комплексі F4AUi254a/1 в зазначений нижче час.

2018	Час входу	Час виходу
28 червня	13:16:52	13:35:24

26 червня	13:13:11	13:40:38
12 червня	13:09:22	13:29:08
22 травня	13:03:12	13:40:32
8 травня	12:55:25	13:56:10

Антена CallmeUa F4AUi254a/1 розташована в будівлі Національного транспортного університету на вулиці Лаврська та спрямована на південний схід.



Як показано на карті, Парк Вічної Слави розташовано в центрі зони, яку покриває антена CallmeUa F4AUi254a/1

Виходячи із вказаного, прокурор вважає, що цих доказів достатньо для підтвердження зустрічей Недовірятенка та Коджошуа в зазначений час.

Однак захист оспорює ці докази та вказує, що жодних зустрічей не було.

++++++++++++++++++

Питання:

Захист просить викликати спеціаліста для допиту.

Чи ставили б Ви питання захисту перед вирішенням клопотання?

Якщо так, то які?

У разі задоволення клопотання, які питання можна поставити спеціалісту при допиті?

Які недоліки мають дані стільникового зв'язку та геолокації як докази місцезнаходження особи?

Які факти та обставини можуть підтвердити позицію захисту, що Недовірятенко та Кожошуа не зустрічались?

Чи вважаєте Ви такі докази достатніми для висновку про зустрічі полковника Петра Недовірятенка та Джеррі Кожошуа?

Додаток 2. Практична вправа щодо перевірки дотримання процесуального закону при вилученні пристроїв та при подальших діях з електронними доказами

ПРИМІРНИК СЛУХАЧА

Свідчення лейтенанта поліції Якова Коваленка

1. Я, Яків Коваленко, лейтенант Національної поліції України, місце роботи - вул. Академіка Богомольця, 10, м. Київ, 01601. Рівно о 08:00 25 вересня 2018 року я прийшов за адресою: проспект Нікуди, 14, м.Київ, і я зараз знаю, що це помешкання полковника Петра Недовірятенка. Я працював у складі групи на чолі з капітаном поліції В. Онтко. У приміщенні була доросла жінка, яку я зараз знаю як дружину підозрюваного, Ірена Недовірятенко, і підліток, якого я зараз знаю як сина підозрюваного, Дем'ян Недовірятенко.

2. Відповідно до ухвали слідчого судді я вилучив з приміщення, яке належить Недовірятенку, ноутбук Apple Macbook срібного кольору, настільний комп'ютер Dell XPS та Apple iPhone 8.

3. Настільний комп'ютер Dell XPS був у невеликій кімнаті, яка, вочевидь, використовувалася як кабінет. На момент прибуття підозрюваний користувався настільним комп'ютером. Перш ніж виймати кабелі позаду ПК і взяти його під варту, я наказав йому вимкнути комп'ютер у безпечний спосіб.

4. Співробітники супроводжували підозрюваного до відділку, поки я заносив до переліку і позначав вилучене обладнання. Я передав копію цього переліку пані І. Недовірятенко. Потім я відніс речі до відділу поліції та зареєстрував їх. Коли я реєстрував iPhone, він задзвонив. Я записав номер (0574838291), натиснув кнопку «Відповісти» і почав слухати. Це був чоловік, який розмовляє англійською з американським акцентом. Я не розмовляю англійською, але я дізнався ім'я – Петро та Парк Вічної Слави. Оскільки телефон був відкритий, я обшукав список контактів та знайшов одне іноземне ім'я, пов'язане з цим номером: Джеррі Коджошуа.

++++++++++++

Запитання:

Оцініть дії на місці злочину. Що було зроблено належним чином? Що можна було зробити ліпше?

Чи мав слідчий право відповідати на телефонний дзвінок?

Які можливі наслідки перевірки телефонних контактів?

Які фактори впливають на допустимість цих доказів?

Які запитання ви б поставили Я. Коваленку?

Додаток 3. Практична вправа із оцінки використання електронних доказів

ПРИМІРНИК УЧАСНИКА

Прокурор Старознаменської місцевої прокуратури звернувся до слідчого судді місцевого суду з клопотанням, про тимчасовий доступ до документів та речей по кримінальному провадженню, внесеному до Єдиного реєстру досудових розслідувань за №12017240220000333, відомості про яке внесено до Єдиного реєстру досудових розслідувань «14» лютого 2017 року за ч. 1 ст. 361, ч. 3 ст. 191, ч. 1 ст. 366 КК України.

В ході досудового розслідування встановлено, що за допомогою комп'ютерної програми «Anyplace Control», яка була попередньо встановлена на комп'ютер (при невідомих органом досудового розслідування обставинах), яким здійснюється ведення бухгалтерського обліку ТОВ «Старцукор», зокрема за допомогою електронного підпису в програмному забезпеченні «M.E.D.O.K.», в режимі реального часу, через мережу «Інтернет», з використанням вказаної комп'ютерної програми, яка дозволяє віддалено працювати з комп'ютером, було проведено несанкціоноване втручання в роботу автоматизованої системи реєстрації податкових накладних в ЄДРПН та від імені ТОВ «Старцукор» було зареєстровано вісім податкових накладних про надання послуг підприємству ТОВ «Легал » на загальну суму 20000000 грн., внаслідок чого сталося зменшення реєстраційного ліміту ПДВ ТОВ «Старцукор» на загальну суму 3333333,33 грн., які в подальшому перераховано ТОВ «Шеваль Гранд», ТОВ «Білгороденерго», ТОВ "АПТ-Україна" та іншим суб'єктам господарювання.

Проведеним досудовим розслідуванням встановлено, що реєстраційний ліміт ПДВ ТОВ «Старцукор» на загальну суму 3333333,33 грн. було перераховано шляхом реєстрації податкових накладних по ланцюгу ТОВ «Старцукор» → ТОВ «Легал » → ТОВ «Шеваль гранд» → ТОВ «Білгороденерго».

При реєстрації податкових накладних вказаними суб'єктами господарювання використовувалась однакова IP-адреса 46.101.245.86 та електронні поштові скриньки:

ТОВ «Легал фін груп» - legal@ukr.net та serg_02@ukr.net

ТОВ «Шеваль гранд» - sheval@ukr.net

ТОВ «Білгороденерго» - bilgorod@ukr.net

Розпорядником (володільцем) сервісу електронної пошти Freemail (mail.ukr.net) з розширенням @ukr.net є ТОВ «Укрнет», код ЄДРПОУ 25589169, юридична адреса - 03039, м.Київ, Голосіївський проспект, буд.26.

Враховуючи викладене, виникла необхідність в отриманні тимчасового доступу до відомостей по вказаних електронних поштових скриньках.

Прокурор просить надати тимчасовий доступ до:

відомостей про електронні поштові скриньки ТОВ «Легал» - legal@ukr.net, ТОВ «Шеваль гранд» - sheval@ukr.net, serg_02@ukr.net ТОВ «Білгороденерго» - bilgorod@ukr.net, розпорядником яких є ТОВ «Укрнет», зокрема дані, що надаються Користувачем як при заповненні реєстраційних форм Сервісів, так і у процесі користування Сервісами Freemail (mail.ukr.net) згідно з публічними Угодою про використання електронної пошти Freemail

(https://mail.ukr.net/terms_uk.html) та Угодою конфіденційності (https://www.ukr.net/terms/), а саме:

- дані реєстраційної форми (інформація щодо реєстрації поштової скриньки): ім’я, прізвище, дата народження, резервна e-mail адреса, мобільний телефон.

- відомості щодо вхідних/вихідних/видалених електронних повідомлень/спаму/чернеток і комп'ютерних файлів, що зберігаються (зберігались) в електронній поштовій скриньці, надходили/відправлялись з вказаної поштової скриньки, включаючи кореспонденцію, адресну книгу, комп'ютерні файли, іншу інформацію, в тому числі видалену з поштової скриньки, яка є в розпорядженні ТОВ «Укрнет»

- відомості щодо надходження/відправлення та зберігання комп'ютерних файлів у поштовій скриньці в сервісі «E-disk»

- файли cookie для користування поштовою скринькою

- ір-адреси, з яких здійснювалось користування поштовою скринькою

- параметри та налаштування інтернет-браузерів користувача поштової скриньки

Зобов'язати ТОВ «Укрнет», код ЄДРПОУ 25589169, юридична адреса - 03039, м.Київ, Проспект 40-річчя Жовтня (Голосіївський проспект), будинок 26, виготовити на паперовому та/або електронному носії відомості про електронні поштові скриньки ТОВ «Легал фін груп» - legal@ukr.net, ТОВ «Шеваль гранд» - sheval@ukr.net, serg_02@ukr.net ТОВ «Білгороденерго» - bilgorod@ukr.net в період часу з моменту їх створення по дату дії ухвали.

Завдання для слухачів: викладіть резолютивну частину ухвали слідчого судді.

Додаток 4. Практична вправа з оцінки допустимості доказів

ПРИМІРНИК УЧАСНИКА

Як саме ситуації, що наведені нижче, можуть вплинути на допустимість зазначених доказів?

1. Захист стверджує, що відповідач був змушений застосувати ключ шифрування до зашифрованої теки (або архіву) на цьому комп'ютері. Файли, знайдені в теці, були вельми компрометуючими, але докази щодо застосування сили для отримання ключа шифрування відповідача включають:

    a. Часова відмітка в протоколі дачі показів говорить, що протягом кількох хвилин допиту здійснювався доступ (до комп'ютера).

    b. Якийсь відвідувач поліцейського відділку заявив, що під час допиту з кімнати допиту було чутно крики болю, а також голосні крики: «Дай нам пароль!» разом зі звуками ніби хтось вдарився об стіл або підлогу.

2. Захисник (який добре знається на електронних доказах, що є стандартною ситуацією), звертається до суду з копією жорсткого диска, що використовується в доказах, для перегляду висновків іншим експертом. Судовий експерт зізнається, що він забув зробити копію, і зробив тест на оригінальному жорсткому диску.

3. Ви переглядаєте звіт фахівця з цифрових технологій та помічаєте помилку в hash-значеннях. Hash-значення для оригінального диска та копії відрізняються. Ви запитуєте експерта, який не може пояснити цю розбіжність. Він вважає, що це помилка копіювання/вставки.

4. Суду надано докази з комп'ютера №5 бізнес-центру готелю, у приміщенні якого, загалом, 15 комп'ютерів. Жорсткий диск було взято з комп'ютера №5. Прокурор стверджує, що відповідач скористався цим конкретним комп'ютером №5, аби надіслати анонімне електронне повідомлення з пропозицією неправомірної вигоди меру міста в обмін на вигідне бізнес-рішення. Однак:

    a. У момент відправки електронного повідомлення користувалися лише 10 комп'ютерами у бізнес-центрі, але вилучили лише жорсткий диск комп'ютера №5. Захист визнає, що відповідач був у бізнес-центрі, але наполягає на тому, що він використовував зовсім інший комп'ютер.

    b. У криміналістичному звіті зазначено, що одразу ж після відправлення електронного повідомлення був використаний комп'ютер №5 для перевірки щоденного гороскопа знаку зодіаку Козеріг на англомовному веб-сайті. Знак зодіаку підсудного – Овен і, за словами відповідача, він не володіє англійською мовою.

Додаток 5. Практична вправа з питань міжнародного співробітництва щодо отримання та використання електронних доказів

Вправа 1

ПРИМІРНИК УЧАСНИКА

НАЗК під час моніторингу доходів та витрат голови районної державної адміністрації Іваненка О.С. встановило, що ним в поточному році подано заяву про істотні зміни в майновому стані у зв'язку із придбанням будинку вартістю 1 500 000 гривень. Іваненко О.С. перебуває на державній службі понад 5 років і подає щорічні декларації про майновий стан, згідно яких щорічний дохід його родини складає близько 200 000 гривень, а в останній щорічній декларації ним не було вказано ніяких готівкових коштів чи інших грошових збережень. Інформація була передана НАБУ, складено обвинувальний акт за статтею 368-2 КК України, і направлено його до суду.

Під час судового розгляду захист пояснив, що Іваненко О.С. має неверифікований акаунт на букмекерському сайті 1xBet, який розташований в Австрії. В період після подання декларації та до придбання будинку Іваненко О.С. активно робив ставки на спортивні заходи, і часто вигравав суми, які не підлягають окремому декларуванню в межах від 30 000 до 70 000 гривень, і його загальний дохід, з урахуванням програшів, становить близько 2 000 000 гривень.

Захист подав клопотання про направлення запиту до букмекерської контори в Австрії та витребування даних щодо акаунту, зокрема часу сесій зв'язку, загальної статистики виграшів/програшів в період за останній рік, та IP адрес, з яких здійснювалось підключення.

Питання для слухачів:

1. Чи вважаєте Ви клопотання таким, що підлягає задоволенню?

2. Враховуючи, що акаунт неверифіковано, яким чином можна встановити його належність саме Іваненку О.С.? Які ще відомості необхідно витребувати і з якої організації після отримання відповіді на запит?

3. У разі задоволення клопотання, якою Конвенцією про міжнародну допомогу буде найбільш доцільно скористатись?

4. У разі направлення запиту та отримання даних, які підтверджують аргумент захисту, чи вважаєте Ви такі докази достатніми для ухвалення виправдувального вироку у справі?

Вправа 2

ПРИМІРНИК УЧАСНИКА

Слідчий Петренко О.П. обвинувачується у вимаганні та одержанні неправомірної вигоди, за ч. 3 ст. 368 КК України.

Яковенко І.С. пояснив, що слідчий Петренко О.П. під час його допиту в якості обвинуваченого в іншому кримінальному провадженні запропонував закрити справу щодо Яковенко І.С. за неправомірну вигоду у розмірі 4 000 доларів США.

Яковенко І.С. погодився, та одразу звернувся до правоохоронних органів з відповідною заявою.

Йому надали грошові кошти, помічені спеціальною хімічною речовиною, для передачі слідчому, а також надали диктофон та відеокамеру, вбудовану у барсетку для здійснення аудіо та відео фіксації передачі.

Яковенко І.С. пояснив, що в кутку кабінету слідчого є металевий сейф. Коли він зайшов до кабінету, то одразу поставив барсетку на стіл слідчого, камерою до останнього. Але під час розмови слідчий раптово піднявся, підійшов до нього та написав на аркуші паперу, що гроші слід покласти до сейфа. Ці дії на камері зафіксовано не було, і слідчий нічого не говорив вголос.

Яковенко І.С. поклав гроші в сейф та вийшов. Через годину в кабінеті слідчого провели обшук, під час якого знайшли помічені гроші в сейфі.

Слідчий на досудовому розслідуванні від надання пояснень відмовився на підставі ст. 63 Конституції України.

Обвинувальний акт направлено до суду.

Під час судового розгляду слідчий Петренко О.П. пояснив, що ніяких грошей не вимагав та не брав, і у прокурора взагалі немає ніяких доказів вимагання та отримання ним грошей, крім самого факту їх вилучення у нього в кабінеті під час обшуку. Але у нього в кабінеті, на стелі була встановлена його власна відеокамера, яка здійснювала безперервний відеозапис всіх подій в день обшуку із збереженням запису на Хмару. В день обшуку, після проведення допиту Яковенко І.С. та до початку обшуку минула година, протягом якої він декілька разів виходив з кабінету на невеликі проміжки часу, не зачиняючи його. Ймовірно, гроші підкинули йому в такий період. Він їх вперше побачив під час обшуку.

Під час обшуку у нього вилучили відеокамеру, але вона не обладнана зберігаючим пристроєм, а запис зберігається безпосередньо на хмарному сервісі Alps Host, який розташований в Німеччині. Він не може самостійно надати цей запис, оскільки пароль від акаунту на хмарному сервісі був записаний у блокноті, який також був вилучений під час обшуку, і він, побоюючись, що його паролем скористується слідство для знищення доказів, негайно звернувся до компанії Alps Host з повідомленням про втрату пароля та попросив заблокувати дані на його акаунті.

Захист просить суд направити запит про міжнародну правову допомогу до Німеччини та витребувати відеозапис за день обшуку у власника хмарного сервісу зберігання даних.

Питання для слухачів:

1. Чи вважаєте Ви клопотання таким, що підлягає задоволенню?

2. У разі задоволення клопотання, якою Конвенцією про міжнародну допомогу буде найбільш доцільно скористатись?

3. Який порядок направлення такого запиту про міжнародну допомогу?

4. Чи була сторона захисту зобов'язана повідомити прокурору про наявність такого доказу при відкритті матеріалів?

15.2 Перелік презентацій

- **Додаток 6**: Презентація до лекції «Природа електронних доказів» (в окремому файлі)
- **Додаток 7**: Презентація до лекції «Мережа Інтернет: принципи функціонування» (в окремому файлі)
- **Додаток 8**: Презентація до практичної вправи щодо використання даних геопозиції та координат базових станцій для визначення місцезнаходження особи в певний час та використання цих даних в якості доказів у кримінальному провадженні
- **Додаток 9**: Презентація до лекції «Судова експертиза електронних доказів»
- **Додаток 10**: Презентація до лекції «Способи виявлення прихованих файлів»
- **Додаток 11**: Презентація до лекції «Основні засади законодавчого регулювання електронних доказів в Україні»
- **Додаток 12**: Презентація до міні-лекції «Критерії допустимості електронних доказів»
- **Додаток 13**: Презентація до міні-лекції «Технічні та юридичні особливості криптовалюти»
- **Додаток 14**: Презентація до лекції «Міжнародне співробітництво при зборі електронних доказів»