Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Цифрова криміналістика

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«26» серпня 2024 р.

Розробник (-и): Ларченко М.О., доцент, кандидат юридичних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2024 р. № 7

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	українська
Рік навчання та семестр	2024-2025 навчальний рік, ІІ семестр, ОП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології
Викладач (-і)	Ларченко Марина Олександрівна, доцент кафедри кібербезпеки та математичного моделювання, кандидат юридичних наук.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38067 296 74 99, E-mail: urlinka2006@gmail.com

2. Анотація курсу.

Дисципліна **"Цифрова криміналістика"** є вибірковою частиною програми підготовки магістрів ОП **Кібербезпека** за спеціальністю 125 **Кібербезпека та захист інформації**, галузь знань 12 **Інформаційні технології**. Курс надає фундаментальні знання та практичні навички з аналізу цифрових доказів, методів їх збору, збереження та дослідження.

Загальна тематика курсу охоплює: принципи та методи цифрової криміналістики; міжнародні стандарти та правові аспекти проведення цифрових розслідувань (ISO/IEC 27037, NIST, ДСТУ тощо); технічні методи виявлення, вилучення та аналізу цифрових доказів; криміналістичний аналіз операційних систем, мобільних пристроїв і мережевих середовищ; виявлення та розслідування кіберзлочинів, зокрема злому, шахрайства, шкідливого програмного забезпечення; використання спеціалізованих інструментів для цифрової криміналістики (Autopsy, EnCase, FTK, Volatility тощо).

Підхід до викладання орієнтований на поєднання теоретичних основ та практичних кейсів, включаючи аналіз реальних кіберінцидентів. Значна увага приділяється розвитку аналітичного мислення, роботи з цифровими доказами та підготовці експертних висновків.

Курс готує спеціалістів, здатних професійно виконувати технічні процедури розслідування кіберзлочинів, використовувати сучасні криміналістичні інструменти та застосовувати правові норми у сфері цифрової криміналістики.

3. Мета та цілі курсу.

Мета курсу – формування у студентів системного розуміння цифрової криміналістики, розслідування кіберзлочинів та аналізу цифрових доказів, а також розвиток практичних навичок використання спеціалізованого програмного забезпечення для збору, обробки та експертизи цифрових даних.

Цілі курсу:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КЗ 6. Здатність до ініціативності, відповідальності та навички до превентивного і аварійного планування, управління заходами безпеки професійної діяльності, уміння приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості та знання міжнародних норм і законодавства України у сфері безпеки життєдіяльності населення, системи управління охороною праці та цивільного захисту

КФ 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

4. Результати навчання:

ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації,прогнозування та прийняття рішень.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

5. Пререквізити. Вміння застосовувати стандарти сертифікації для оцінки ефективності засобів захисту інформації; навички в управлінні ризиками та проведенні аудиту безпеки в контексті сертифікації.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин
Лекції	16/6
Практичні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, практичні заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16/6 годин):

1. **Вступ до цифрової криміналістики та її правові основи** (2 години)
   Поняття, завдання та принципи цифрової криміналістики.
   Основні терміни та концепції: цифрові докази, ланцюг збереження доказів.
   Міжнародні та національні правові аспекти проведення цифрових розслідувань (ISO/IEC 27037, Будапештська конвенція, законодавство України).
2. **Методологія збору та збереження цифрових доказів** (2 години)
   Принципи збору цифрових доказів відповідно до міжнародних стандартів.
   Технології вилучення даних з носіїв інформації (HDD, SSD, USB, мобільні пристрої).
   Створення криміналістичних копій та контроль цілісності доказів (хешування, використання write-blocker).
3. **Криміналістичний аналіз файлових систем** (2 години)
   Структура та особливості файлових систем (NTFS, FAT, ext, HFS+).
   Відновлення видалених файлів та аналіз метаданих.
   Аналіз прихованих та зашифрованих даних.
4. **Дослідження операційних систем у цифровій криміналістиці** (2 години)
   Аналіз артефактів Windows (реєстр, журнал подій, Prefetch, $MFT).
   Особливості аналізу Linux та macOS у криміналістичних розслідуваннях.
   Виявлення слідів діяльності користувача та роботи шкідливого ПЗ.
5. **Мережева криміналістика та аналіз трафіку** (2 години)
   Методи збору та аналізу мережевого трафіку (Wireshark, Zeek, Suricata).
   Виявлення атак, вторгнень та несанкціонованого доступу.
   Аналіз логів мережевих пристроїв, виявлення ознак злому.
6. **Криміналістика мобільних пристроїв** (2 години)
   Методи вилучення та аналізу даних з iOS та Android.

Аналіз журналів викликів, SMS, месенджерів та геолокаційних даних.
Відновлення видалених даних та дослідження мобільного трафіку.

7. **Аналіз шкідливого програмного забезпечення** (2 години)
   Методи ідентифікації та дослідження вірусів, троянів, руткітів.
   Динамічний та статичний аналіз шкідливого коду.
   Виявлення ознак компрометації системи та шляхів зараження.
8. **Складання криміналістичних звітів та представлення доказів у суді** (2 години)
   Стандарти підготовки цифрових доказів для судових процесів.
   Методика написання експертного висновку.
   Презентація цифрових доказів у суді та етичні аспекти роботи експерта.

Практичні (16/6 годин):

1. Практична робота №1: **Криміналістичний аналіз та верифікація відео.**
2. Практична робота №2: **Застосування процедур OSINT.**
3. Практична робота №3: **Дослідження веб-серверу.**
4. Практична робота №4: **Мережевий сніффінг.**
5. Практична робота №5: **IP і MAC-адреса.**
6. Практична робота №6: **Вилучення, передача та аналіз дампів (зліпків) пам'яті.**
7. Практична робота №7: **Перевірка жорсткого диска.**
8. Практична робота №8: **Виявлення фішингу та візуалізація легітимності.**

Розрахунково-графічна робота (РГР)

Тема: Аналіз файлової системи та журналів.

1. Аналіз головного завантажувального запису.

2. Головна таблиця розділів. Отримання доступу до головної таблиці розділів та до головного завантажувального запису.

3. Головна таблиця файлів. Спеціальні інструменти аналізу MFT.

4. Системні журнали. Журнали подій Windows. Системні журнали Linux. Історія командного рядка.

5. Аналіз хронології: Autopsy, Plaso, Timesketch.

Самостійна робота (88/108 годин):

1. **Ознайомлення з нормативно-правовою базою цифрової криміналістики** (10 годин)
   Вивчення міжнародних стандартів (ISO/IEC 27037, NIST, RFC) та національного законодавства України.
   Аналіз положень Будапештської конвенції та їх застосування у цифрових розслідуваннях.
2. **Дослідження сучасних методів вилучення та аналізу цифрових доказів** (12 годин)
   Самостійне опрацювання матеріалів щодо технологій криміналістичного вилучення даних.
   Вивчення принципів write-blocking, хешування та створення судово-медичних копій.
3. **Аналіз файлових систем та відновлення даних** (12 годин)
   Дослідження архітектури файлових систем (NTFS, FAT, ext4, APFS).
   Практичне використання інструментів для аналізу файлових систем (Autopsy, FTK Imager).
4. **Дослідження артефактів операційних систем** (10 годин)
   Аналіз Windows Registry, Prefetch, Pagefile та журналів подій.
   Самостійна робота з PowerShell та інструментами аналізу Windows/Linux.
5. **Збір та аналіз мережевого трафіку** (10 годин)
   Вивчення принципів роботи Wireshark, Zeek, Suricata.
   Самостійне дослідження логів трафіку та виявлення аномалій.
6. **Цифрова криміналістика мобільних пристроїв** (10 годин)
   Ознайомлення з методами аналізу даних iOS та Android.

Практичне опрацювання програмного забезпечення для дослідження мобільних пристроїв (Cellebrite, MOBILedit).

7. **Дослідження шкідливого програмного забезпечення** (12 годин)
   Вивчення методів аналізу шкідливого коду: динамічний та статичний аналіз.
   Робота з середовищами пісочниці (Cuckoo Sandbox) та реверс-інжинірингом.
8. **Підготовка криміналістичних звітів та презентація цифрових доказів** (12 годин)
   Ознайомлення з методикою складання експертних висновків.
   Самостійна підготовка криміналістичних звітів на основі досліджених кейсів.
9. Підготовка до лабораторних занять та виконання тестових завдань.
10. Робота з дистанційними навчальними матеріалами (Moodle, Teams).

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	**Критерії оцінювання РГР:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні (лабораторні) заняття	Оцінка кожного лабораторного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% лабораторних робіт** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю. 3. Виконання **розрахунково-графічної роботи** (РГР).

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів
Змістовий модуль 1. Основи цифрової криміналістики та робота з цифровими доказами		**30/30**
1	Вступ до цифрової криміналістики та її правові основи.	**5/5**
2	Методологія збору та збереження цифрових доказів	**5/5**
3	Криміналістичний аналіз файлових систем	**5/5**
4	Дослідження операційних систем у цифровій криміналістиці	**15/5**
Змістовий модуль 2. Спеціалізовані методи цифрових розслідувань		**30/30**
1	Мережева криміналістика та аналіз трафіку.	**5/5**

2	Криміналістика мобільних пристроїв	**15/15**
3	Аналіз шкідливого програмного забезпечення	**5/5**
4	Складання криміналістичних звітів та представлення доказів у суді	**5/5**
Усього поточний і проміжний модульний контроль		**60/60**
Семестровий контроль (Екзамен)		**40/40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апаратне забезпечення:

Персональні комп'ютери або ноутбуки з підтримкою віртуалізації та можливістю роботи з образами дисків та цифровими доказами.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux – для аналізу вразливостей), macOS.

Серверне обладнання для моделювання атак, аналізу мережевого трафіку та логів.

Мережеве обладнання (маршрутизатори, комутатори, мережеві екрани) для дослідження атак та аналізу цифрових слідів.

Зовнішні накопичувачі (HDD, SSD, USB-флешки) для роботи з криміналістичними копіями та створення дампів пам'яті.

Мобільні пристрої (Android, iOS) для дослідження мобільної криміналістики.

Окремо слід виділити використання **віртуальної машини CAINE (Computer Aided INvestigative Environment)** – спеціалізованого дистрибутиву Linux, що містить інструменти цифрової криміналістики, зокрема для вилучення, аналізу та документування цифрових доказів.

ІІ. Програмне забезпечення:

1. Для збору та збереження цифрових доказів:

FTK Imager – створення криміналістичних копій дисків.

Autopsy, Sleuth Kit – аналіз файлових систем та структури дисків.

Guymager – криміналістичне копіювання дисків у Linux.

2. Для аналізу файлових систем та метаданих:

X-Ways Forensics – глибокий аналіз файлових систем, відновлення даних.

ExifTool – витягнення метаданих із файлів (зображень, документів, відео).

Bulk Extractor – автоматичний пошук артефактів у файлах (номери кредитних карт, паролі).

3. Для дослідження операційних систем та лог-файлів:

Registry Explorer – аналіз реєстру Windows.

Event Log Explorer – дослідження журналів подій Windows.

Plaso, Timesketch – створення хронологій подій на основі логів системи.

4. Для мережевої криміналістики та аналізу трафіку:

Wireshark – аналіз мережевого трафіку.

Zeek (Bro IDS) – моніторинг і розслідування мережевих атак.

NetworkMiner – вилучення артефактів із трафіку.

5. Для криміналістики мобільних пристроїв:

MOBILedit Forensic – вилучення даних із мобільних пристроїв.

Oxygen Forensic Detective – аналіз дзвінків, повідомлень, геолокаційних даних.

Cellebrite UFED – відновлення та аналіз даних із мобільних телефонів.

6. Для аналізу шкідливого програмного забезпечення:

IDA Pro – дизасемблювання та аналіз шкідливого коду.

PE Explorer – дослідження виконуваних файлів Windows.

Cuckoo Sandbox – динамічний аналіз підозрілих файлів у віртуальному середовищі.

7. Для складання криміналістичних звітів та документування:

LaTeX, MS Word – підготовка технічної документації та звітів.

CaseNotes – ведення криміналістичних нотаток.

8. Платформи для дистанційного навчання:

Moodle, Microsoft Teams – розміщення навчальних матеріалів, тестування та проведення лекцій.

Google Drive, OneDrive – спільна робота з документами та звітами.

Використання наведеного обладнання та програмного забезпечення дозволяє студентам отримати практичний досвід у сфері цифрової криміналістики та підготуватися до роботи в реальних криміналістичних розслідуваннях.

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ “Чернігівська політехніка”». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через

вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базові підручники:

1. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина. Київ: 7БЦ, 2023. 512 с.

2. Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews. Received January 22, 2022, accepted February 16, 2022, date of publication February 24, 2022, date of current version March 10, 2022. URL: https://www.researchgate.net/publication/358837101_Research_Trends_Challenges_and_Emergin_Topics_in_Digital_Forensics_A_Review_of_Reviews

3. Tarun Vashishth. Cyber Forensics Up and Running. A hands-on guide to digital forensics tools and technique. Published by BPB Online WeWork, 2024. 407 p.
4. eForensics Magazine. Workshop. URL: https://eforensicsmag.com/.
5. Bruce Middleton. Cyber Crime Investigator's Field Guide. Third Edition. Chennai, India: CRC Press, 2022. 353 p.
6. Introduction to Forensic and Criminal Psychology. 7th Edition. Dennis Howitt Loughborough University. New York: Pearson Education Limited, 2022. 768 p.

Джерела:

1. ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf
2. Репозиторії готових дампів па'яті для аналізу на гітхаб. URL: https://github.com/SecurityNik/CTF, https://github.com/cyph3rryx/Kryptonite-RAM-Dump-Collection, https://www.baeldung.com/linux/dump-memory-image, https://github.com/504ensicsLabs/LiME
3. Образ віртуальної машини Caine, що містить необхідні інструменти в галузі Computer Forensics. URL: https://www.caine-live.net/page5/page5.html
4. Образ віртуальної машини Kali Linux. URL: https://www.kali.org/get-kali/#kali-platforms
5. Платформа для візуалізації та емуляції на MacOS. URL: https://mac.getutm.app/
6. Власний репозиторій з програмним інструментом для трансферу дампів пам'яті в ізольований контейнер Caine для аналізу. URL: https://github.com/urlinka2006/CyberInsight
7. Autopsy – платформа цифрової криміналістики та графічний інтерфейс для The Sleuth Kit та інших інструментів цифрової криміналістики. URL: https://github.com/sleuthkit/autopsy
8. WireShark – найпопулярніший у світі аналізатор мережевих протоколів. URL: https://www.wireshark.org/
9. Sleuth Kit (TSK) – бібліотека та колекція інструментів цифрової криміналістики командного рядка, які дозволяють досліджувати томи та дані файлової системи. Бібліотеку можна включити до більших інструментів цифрової криміналістики, а інструменти командного рядка можна безпосередньо використовувати для пошуку доказів. URL: https://github.com/sleuthkit/sleuthkit
10. BelkaGPT — перший автономний AI-помічник для розслідувань DFIR. URL: https://belkasoft.com/belkagpt?utm_campaign=Police%201&utm_source=Media&utm_medium=Article&utm_term=eforensicsmag&utm_content=belkagpt