

# THE CUTTING EDGE OF A DOUBLE-EDGED SWORD

AI in Action for Law Enforcement





# BEFORE WE START

**DISCLAIMER**

- Opinions are our own and do not necessarily express the opinion or formal position of the Netherlands Police or any other entity
- Fair Use Notice and Disclaimer – all material in this presentation is for not-for-profit use and is only intended for educational purposes
- Some pictures in this presentation are generated by AI
- Errors may occur

# Presenters

---

Jonathan Lewin



Oscar Wijnsman



Changlin Li



# LEARNING OBJECTIVES



1. Identify key AI technologies relevant to policing, assess their benefits and risks, and develop strategies for implementing AI responsibly to address real-world problems to improve outcomes within agencies, regardless of agency size or budget.
2. Develop actionable strategies for integrating AI into agencies, establish safeguards to mitigate risks such as bias and misuse, and align AI policies with legal and ethical frameworks.
3. Detect AI-generated threats such as deepfakes and synthetic media, analyze potential security vulnerabilities, and apply countermeasures to protect their agencies from AI-driven fraud, cybercrime, and misinformation campaigns.

# 2026 - A transformational year

Not just another milestone - AI will fully transform core aspects of policing:

- Convergence of advanced technologies widespread adoption
- Transformative impacts across law enforcement

Drivers:

- Technological breakthroughs
  - Next-generation LLMs, VLMs
  - AI agents / Agentic AI
  - New hardware innovations
  - Quantum & Edge AI
- AI has begun to fundamentally change our operational model as well as the business model

# VLM Bootcamp



# The true reason why Italy banned ChatGPT



Can I put pineapple on pizza?

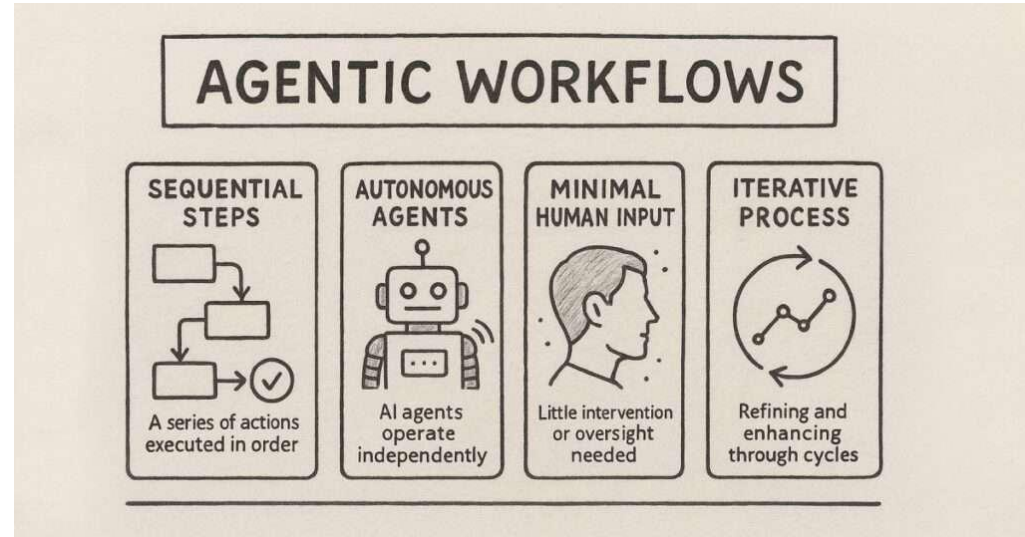


Yes, you can. It's a matter of personal preference.

# Agentic AI : Beyond the hype

Agentic AI is a broad term that includes

- systems
- platforms
- practices
- tools
- technologies



**Execute with minimal human intervention**

**AI agents represent a shift to using a variety of specialized models for different tasks**

# Impact of Agentic AI : measures

Redesign processes

-> deploy AI agents effectively and reimagining business models

Transform workforce, organizational structure

-> agentic workforce as team members

Strike the right balance

-> between agent autonomy and human involvement

Strengthen data and technological foundations

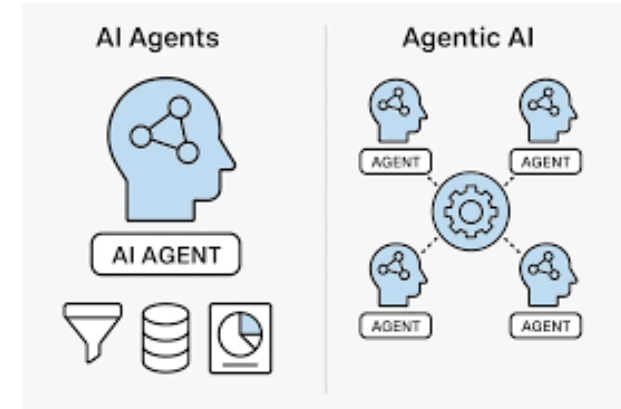
-> to scale AI agents

Ensure AI agents operate

-> within defined scope of execution


-> remain traceable and explainable to earn trust

**Develop and integrate ethical AI that address risks posed by autonomous AI agents**



# Agentic AI - a security risk?

## 5 Real AI Agent Security Breaches in 2026 (And What Each One Teaches Us)

 by Fredrik Falk



88% of organizations running [AI agents](#) reported a confirmed or suspected security incident in the past year. Only 6% of security budgets are dedicated to AI agent security.

# Public discourse on AI

Heightened public discourse on AI continues in 2026 and is even more sparked by widespread concerns over its societal impact

- on democracy – amplifying debates
- real data framed as fake
- use of AI beyond it's intended purpose
- widespread misinformation
- manipulating opinions & fake content
  
- (lack of) transparency how it is used
- lack of federal regulation (in the US)
- who controls essential digital infrastructure



(c) OpenAccesGovernment

# Who can I trust? Falsify the truth

Technical looking analyses  
are being weaponized  
to falsely discredit  
authentic evidence



Low High Map

Likely AI Artifacts

# Human centric, not machines

But we must not forget to recognize  
the irreplaceable value of:

- our professional judgement
- experience and human connection

At the heart of effective and just policing



# Trust remains critical



## The intelligent age has arrived

66% of people use AI regularly, and **83% believe the use of AI will result in a wide range of benefits.**



## Trust remains a critical challenge

Yet, trust remains a critical challenge: only **46% of people globally are willing to trust AI systems.**



## AI regulation

There is a public mandate for national and international AI regulation with **70% believing regulation is needed.**



## AI at work

Many **rely on AI output without evaluating accuracy** (66%) and are making mistakes in their work due to AI (56%).

**There is a distinct divide between mere Technical Acceptance and Genuine Public Trust!**

# Trust remains critical

For organizations to realize the true potential of AI and achieve a competitive advantage, there are four key actions that leaders should prioritize:

01 Transformational leadership

02 Enhancing trust

03 Boosting AI literacy

04 Strengthening governance



[https://mbs.edu/-/media/PDF/Research/Trust\\_in\\_AI\\_Report.pdf](https://mbs.edu/-/media/PDF/Research/Trust_in_AI_Report.pdf)

By acting decisively to address these areas, organizations can not only mitigate current risks but also drive sustainable innovation and growth.



# Trust remains critical



## The intelligent age has arrived

66% of people use AI regularly, and **83% believe the use of AI will result in a wide range of benefits.**



## Trust remains a critical challenge

Yet, trust remains a critical challenge: only **46% of people globally are willing to trust AI systems.**



## AI regulation

There is a public mandate for national and international AI regulation with **70% believing regulation is needed.**



## AI at work

Many **rely on AI output without evaluating accuracy** (66%) and are making mistakes in their work due to AI (56%).

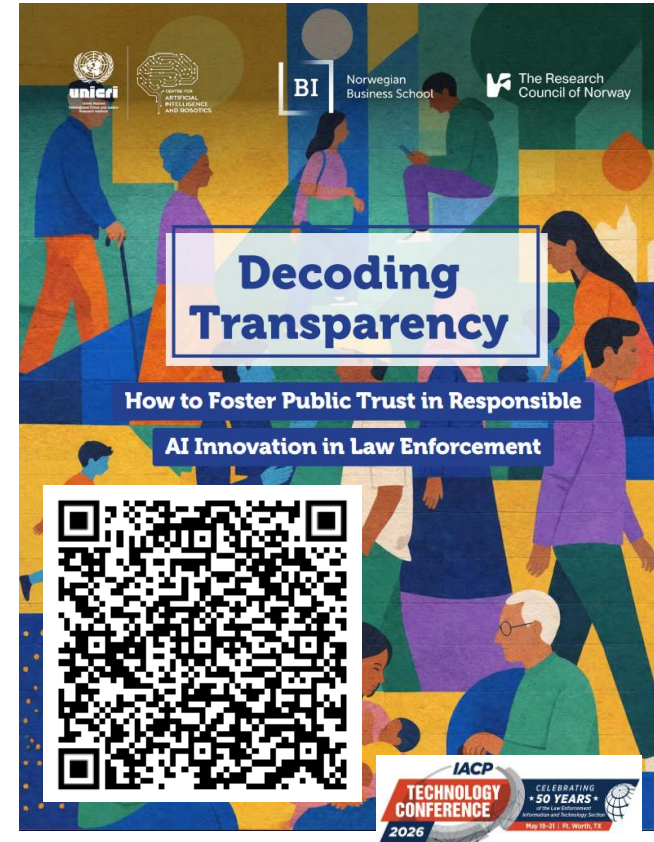
# Public trust is under pressure

## Transparency

- Explaining what AI systems are used and why
- How decisions are made
- What safeguards exist
- Acknowledging risks, limitations and uncertainties
- Space for questions, feedback and dialogue

## Communication

- Engage early, before AI systems are deployed
- Maintaining consistent communication
- Reaching audiences through multiple channels
- Ensuring all groups are included
- Building feedback mechanisms



# AI comes in different flavors

Task focused 'classic' AI

versus

General Purpose AI  
(foundation models, LLMs)



# LEA operational uses

- Real Time Crime Centres – 360 view
- CCTV / ALPR / Sensor Data Analysis - streams
- BWC Analysis
- Investigative Support
- Crime Scene Analysis / Digital Forensics
- Crime scripts
  
- OSINT / Social Media Analysis
- Crime Prediction / Risk Modelling
- Report Writing
  
- UAS (drones) Programs




# LEA supportive uses

- Officer Wellness
- Training – including AR/VR
- Legislation / procedural queries
- Community Engagement
- Application Development
- Coding Assistant : in NL we have 'Cody'
- Financial Reporting
- Business Operations




# Czech Police: AIDA

 BORN DIGITAL Born Digital


- Seznam případů
- Výslech**
- Finanční tok
- Datový tok
- Ukončení případu

DEMO - Case - Č. j. KRPS-123456/TC-2023-011581 : Výslech oznamovatele - Klasifikace, Extrakce atributů, Úvodní dokumentace

### Import výsledku pro zpracování



Vyberte nebo přetáhněte soubor.

 Analyzovat

Popis skutku

Dne 10.1.2023 vystavila Tereza Balíková na portálu VINTED inzerát s nabídkou prodeje dvou šatů za 200 Kč a 250 Kč. Téhož dne ve 21:39 obdržela zprávu od zájemkyně s uživatelským jménem "physs", která vyjádřila zájem o šaty a požádala o telefonní číslo Terezy Balíkové. Po sdělení čísla na telefon 123 456 789 obdržela Tereza Balíková SMS z neznámého čísla s odkazem, který vypadá jako platební brána VINTEDu. Vyplnila údaje své platební karty včetně čísla karty, platnosti a bezpečnostního kódu.

Následně obdržela upozornění z aplikace Komerční banky a.s. o zvýšení limitu pro platby. Reakcí Terezy Balíkové bylo okamžité zrušení změn limitu v internetovém bankovníctví a zablokování účtu a kreditní karty u Komerční banky a.s. Po zablokování zjistila, že z jejího účtu č. 11-2233445566/0100 byly vykonány neoprávněné platby ve výši 308 000 Kč na účty č. 111222333/0100 a č. 111555333/0100. Dále byla zjištěna neoprávněná transakce ve výši 600 000 Kč z jejího druhého účtu č. 123-55555666/0100 na účet č. 11-2233445567/0100, z něhož byly financovány zmíněné neoprávněné platby.

Číslo spisu

KRPS-123456/TC-2023-011581

Klasifikace

IT-PHI PK

Je oznamovatel poškozený?

Ano

Výše škody

308 000 Kč

# Czech Police: AIDA - for cybercrime

AI Digital Assistant: Automated investigation/processing of cybercrime cases, which enables investigators to focus on the most serious offenses.

Next step: all types of criminal cases ('every day' MO)

Now 20.000 criminal offenses, up to 160.000 criminal offenses annually

Fully integrated in the on-premise environment

## Benefits:

- Decrease processing time 40 to 70 % (manual 7,5 hrs., with AIDA 29 mins)
- Reduction of error rate
- Improved analytical capabilities
- Improved communication with e.g. banks, telco's, public prosecutors, etc.

# Luxemburg Police: PULSE

PULSE is a chatbot interacting with an LLM.

Core features:

- Direct LLM interaction via natural language
- File upload capabilities
- A suite of pre-configured tools for specific tasks

Supports a wide range of European languages + languages such as Russian or Chinese

- Developed by Europol Innovation Lab
- Runs on-premise
- Pilot project in Luxembourg – 3000 users

No replacement for a search engine Pilot project 🇯🇪

## Luxembourg pioneers Europol police AI project

Grand Duchy is the first EU country to test AI aiming to relieve police workload, with rollout planned for the end of June



Last December, two classes from the police academy put Pulse through its paces. © Photo credit: Polizei



Steve Remesch  
Reporter

Share

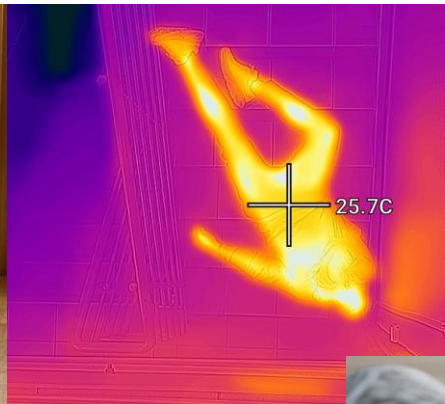
08/06/2025

Luxembourg is taking on a pioneering role in the introduction of artificial intelligence in the police force, developing and testing “Pulse”, a system intended to relieve police forces of everyday tasks.



# Norwegian Police: AI4Interviews

AI 4  
INTERVIEWS



# Norwegian Police: AI4Interviews

Forensic teams spend up to 55% of their time on reporting tasks

- Assisted reality technology to revolutionize Crime Scene Investigation (CSI)
- Supports forensic technicians throughout the entire investigative process
- Smart voice-controlled headsets equipped with assisted reality features

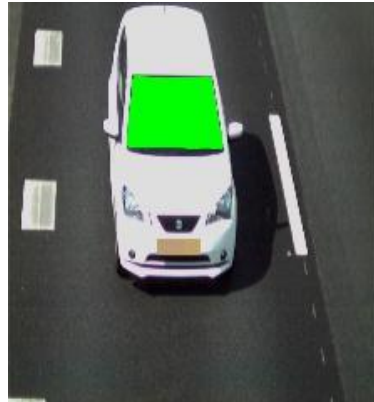
# Netherlands Police: Monocam



# Netherlands Police: Tiresias



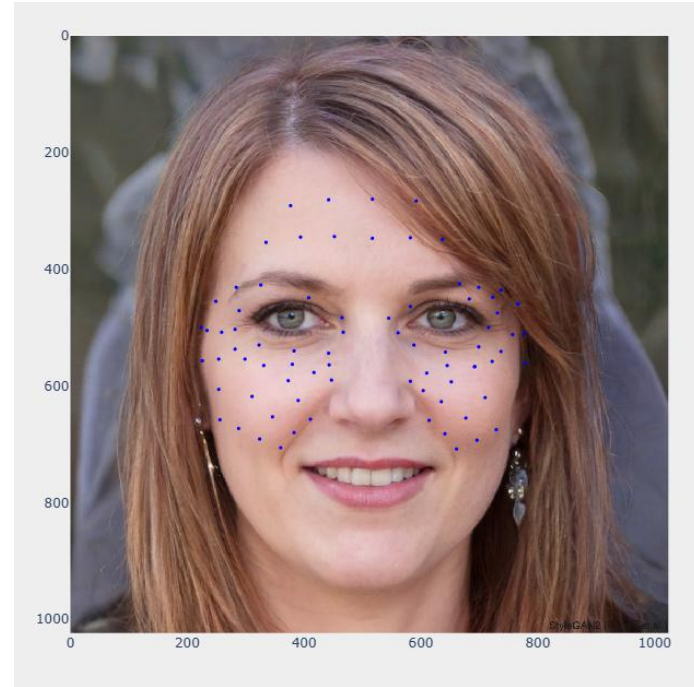
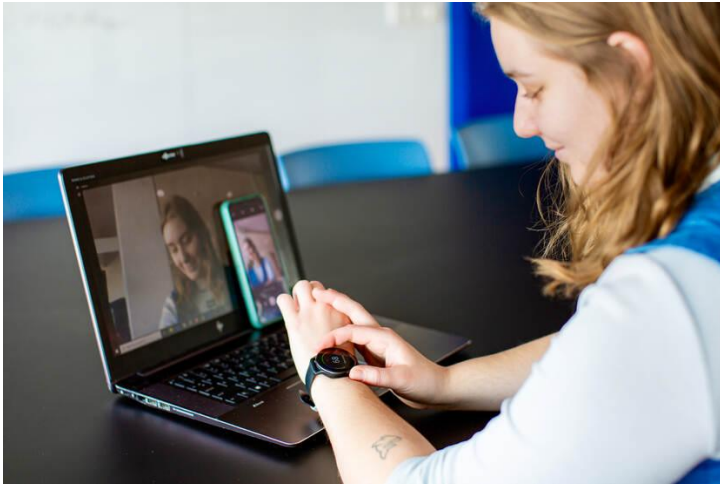
# Netherlands Police: Tiresias



# NFI Deep Fake detector - bloodstream



Nederlands Forensisch Instituut  
Ministerie van Justitie en Veiligheid



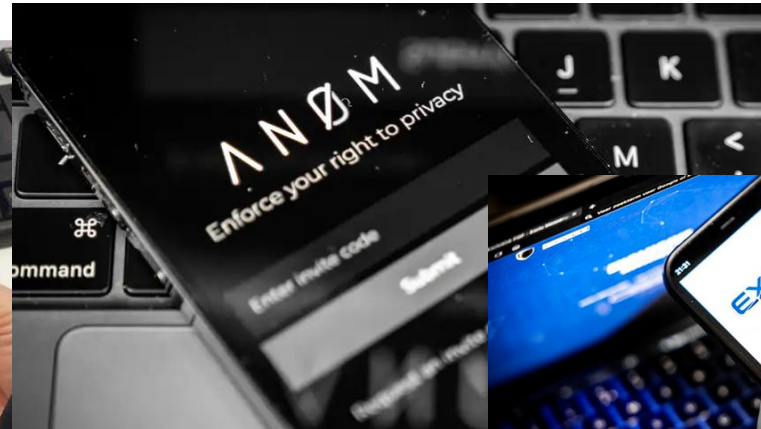
Bloodstream pulse



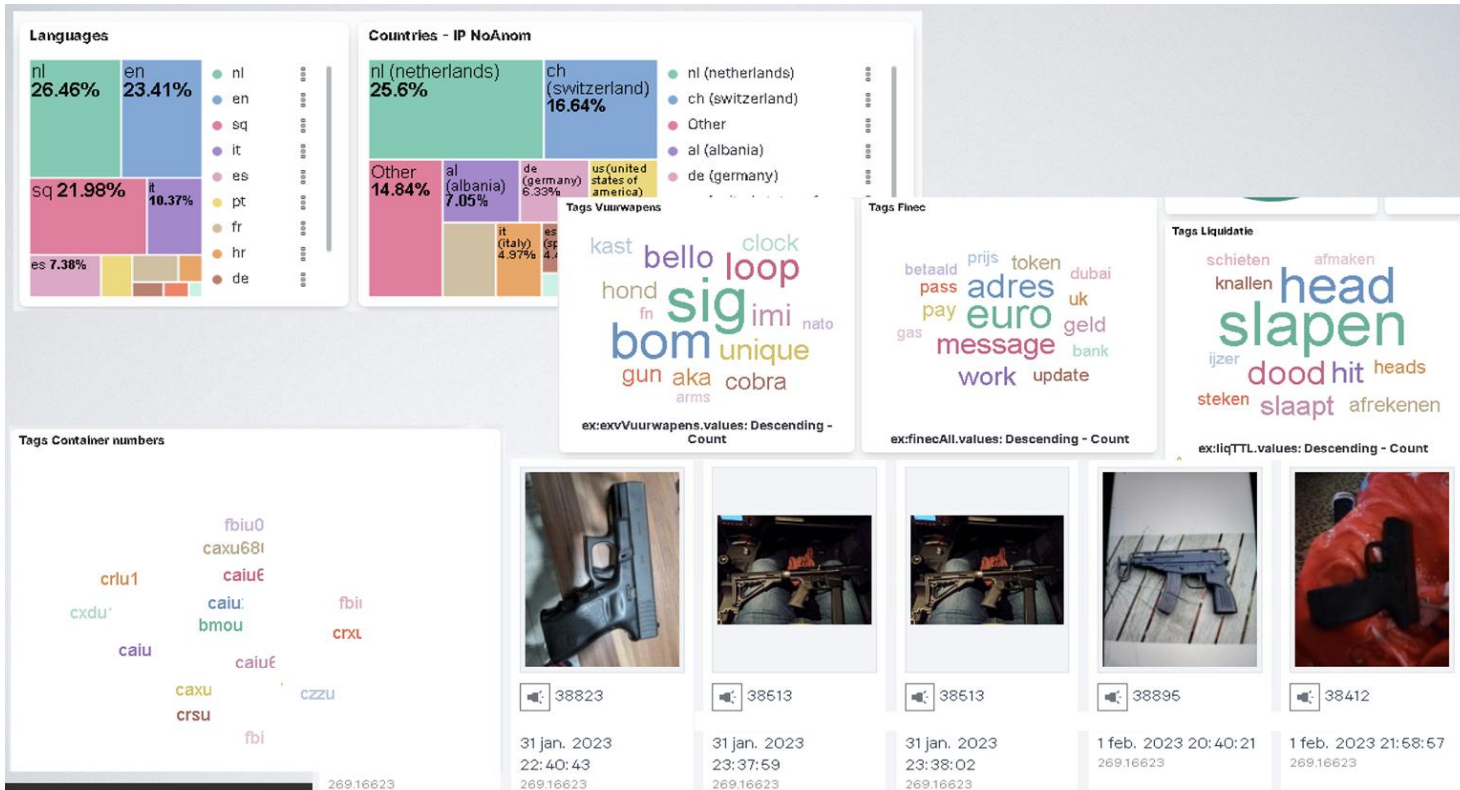
# Cracking crypto data



Ennetcom (2016), PGPSafe, Ironchat (2017), Enchrochat, SkyECC (2020), ANOM (2021), Exclu (2023), Ghost (2024), ...



# Detection, classification



# Europol Tool Repository - ETL

LIST OF TOOLS PROVIDED

Category	Tool Name	Description	Flags
Text processing	SearchBox	Searchbox: index and search for information in very large amount of documents in various formats.	🇺🇦
	Machine translation	Machine translation: translate text in 99 languages.	🇫🇷
	NLP annotator	NLP annotator: extract and visualise entities and relations in text (99 languages supported).	🇫🇷
	KyriellOff	KyriellOff: transliterate names from cyrillic to latin.	🇺🇦
	TRIS	TRIS: extract text from documents with OCR.	🇫🇷
	Erical	Erical: manage and analyse large volumes of seized documents.	🇮🇪
Lang Detector	Lang Detector: identify language of input text, 176 languages supported.	🇺🇦	
PDF2XLSX	PDF2XLSX: conversion of multiple PDF forms into an XLSX file.	🇨🇭	
Image/Video processing	Medusa	Medusa: fast text-2-image and image-2-image search.	🇺🇦
	eVidSteps	eVidSteps: extract persons or vehicles from videos.	🇺🇦
	Face extractor	Face extractor: extract faces from images and videos.	🇺🇦
	VINOME	VINOME: image and video comparison tool.	🇺🇦
Scribe	Scribe: captions images or perform OCR.	🇺🇦	
Image extractor	Image extractor: extract images from PDFs and Word documents.	🇺🇦	
Audio processing	Sendo	Sendo: audio denoising and transcription.	🇺🇦
	Fudge	Fudge: compute how similar are two voices.	🇺🇦
	SeamlessTranslation	SeamlessTranslation: transcribe audio into text and translate text (95 languages).	🇺🇦
SonicTranscriber	SonicTranscriber: simple application for transcription of audio/video file using WhisperV3.	🇺🇦	
Speech-to-text	Speech-to-text: complete application to transcribe audio into text and translate it.	🇫🇷	
Data visualisation	Delata	Delata: analyse large collections of media files for metadata information.	🇺🇦
	PDVizual3D	PDVizual3D: visualise spatial data in a safe, simple, and immersive way.	🇺🇦
HeatPoints	HeatPoints: visualise geolocation data on a map.	🇫🇷	
CEOS	CEOS: visualise BTG data on a map and cross-match with crime dataset.	🇫🇷	
OSINT	Apogee	Apogee: All-Purpose Intelligence Gathering Platform for gathering OSINT scripts.	🇺🇦
	Vision Reconnaissance Monitor	Vision Reconnaissance Monitor: collect, store and analyze information from the ransomware group activities.	🇺🇦
	TAPIS	TAPIS: reconnaissance of Telegram channels / groups / users.	🇩🇪
	ChatExtractor	ChatExtractor: secure content from various messaging platforms.	🇺🇦
	LinkMC	LinkMC: take screenshots of a list of dark/crow web sites.	🇫🇷
GeoTraceTool	GeoTraceTool: geolocate images and find locations based on description.	🇫🇷	
gAIs	gAIs: geolocate street view images (score per country).	🇺🇦	
Crypto investigations	publicator	publicator: analyze extended public keys in Bitcoin and related cryptocurrencies.	🇩🇪
	CryptoScanner	CryptoScanner: search cryptocurrencies addresses, transactions and seed phrases stored in files.	🇩🇪
Password cracking	Lexical	Lexical: generate a list of vocabulary for password cracking based on topics.	🇫🇷
	PassTech	PassTech: generate a dictionary of passwords based on user's inputs.	🇫🇷
Digital forensics	LEKScope	LEKScope: visualise Google subscriber data.	🇩🇪
	FIRST	FIRST: First Responder's Scan Tool.	🇺🇦
	RoastLamb	RoastLamb: artefacts extraction from memory dumps.	🇺🇦
	MemoryMiner	MemoryMiner: data extraction from memory dumps.	🇺🇦
	EVFF	EVFF: analysis of data from vehicle infotainment systems.	🇺🇦
FALSA	FALSA: visualize AnyDesk logs.	🇩🇪	
eMMC examiner	eMMC examiner: read eMMC memory of a device.	🇺🇦	
Data anonymisation	Houdini	Houdini: remove people or other objects from images.	🇺🇦
	Masquerade	Masquerade: anonymise a dataset by obfuscating faces.	🇺🇦
Dataset creation	Platemaster scraper	Platemaster scraper: rapidly build a dataset of license plates with this scraper.	🇺🇦
International cooperation	SiENA constructor	SiENA constructor: speed up and ease the creation of SiENA messages.	🇺🇦
	UMC Viewer	UMC Viewer: visualise UMC data in a human readable way.	🇺🇦

**Text processing**

**Image/Video processing**

**Audio processing**

**Data visualization**

**OSINT**

**Crypto investigations**

**Password cracking**

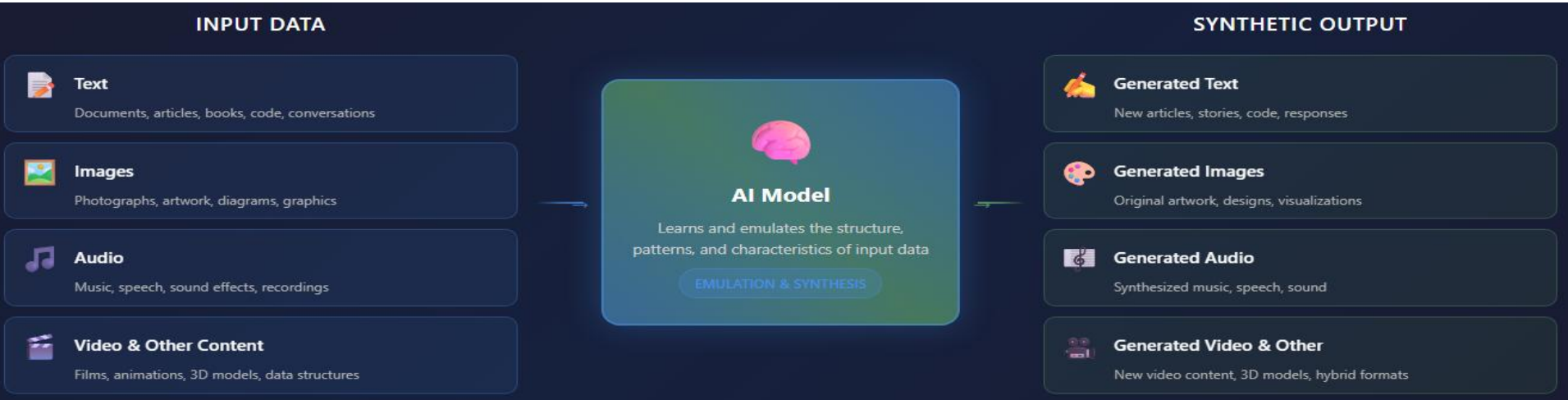
**Digital forensics**

**Data anonymization**

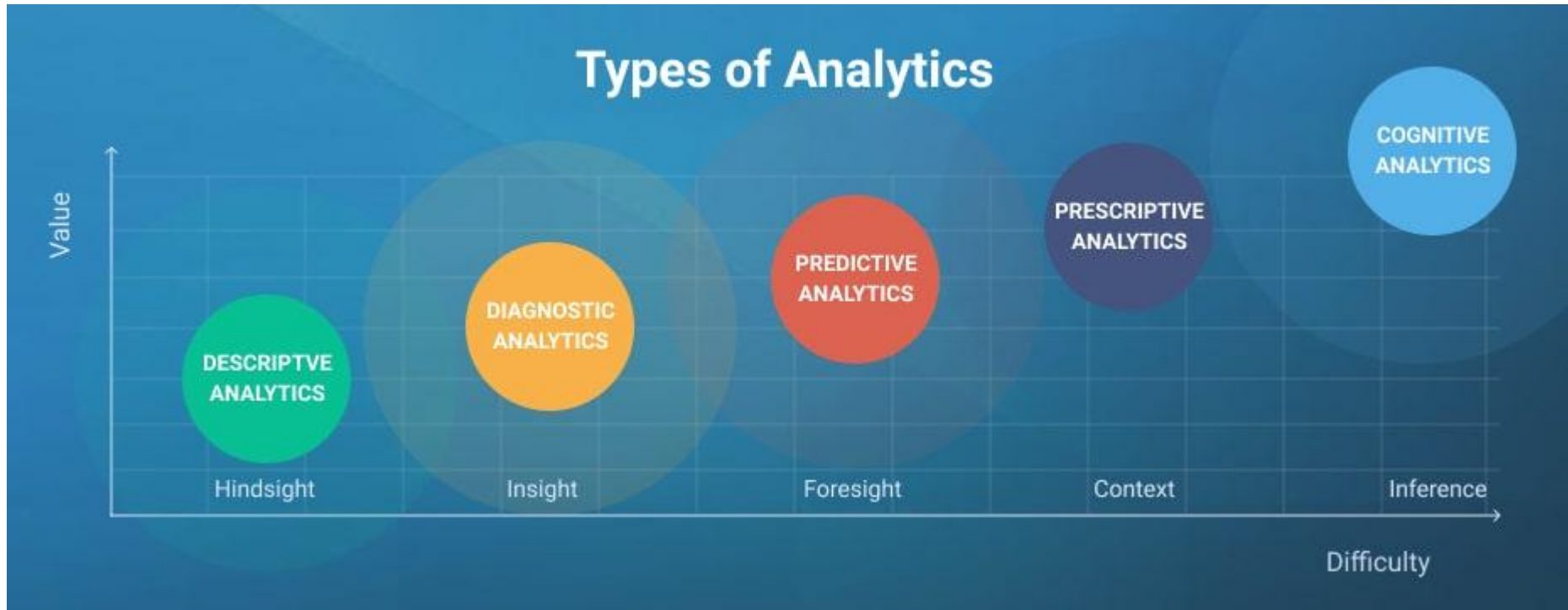


# What is Gen AI ?

"The class of AI models that **emulate the structure and characteristics of input data** in order to **generate derived synthetic content**. This can include images, videos, audio, text, and other digital content."



# A SHORT PRIMER ON GENERATIVE AI



# What Makes Gen AI Different?



## Speed of Adoption

No technology in history has reached mass adoption faster. ChatGPT reached 100 million users in 2 months — before most agencies had even heard of it.

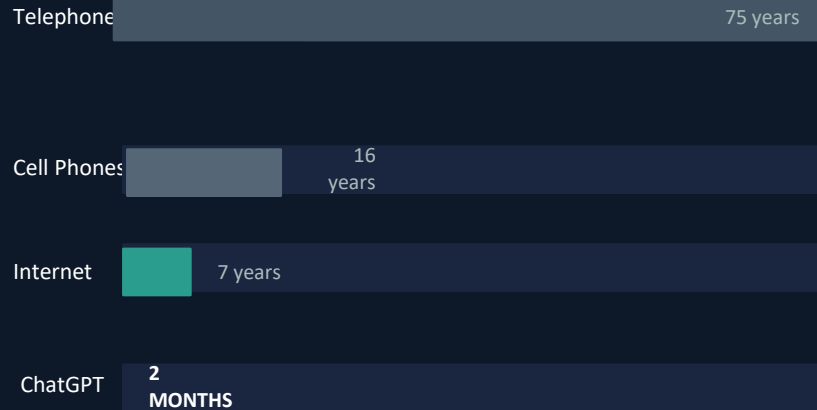
## Zero Barrier to Entry

No training. No installation. No IT department. Any officer with a smartphone can access enterprise-grade AI right now — on or off duty.

## Generates New Content

Unlike previous tools that retrieved or analyzed data, generative AI creates original text, images, analysis, and decisions that never existed before.

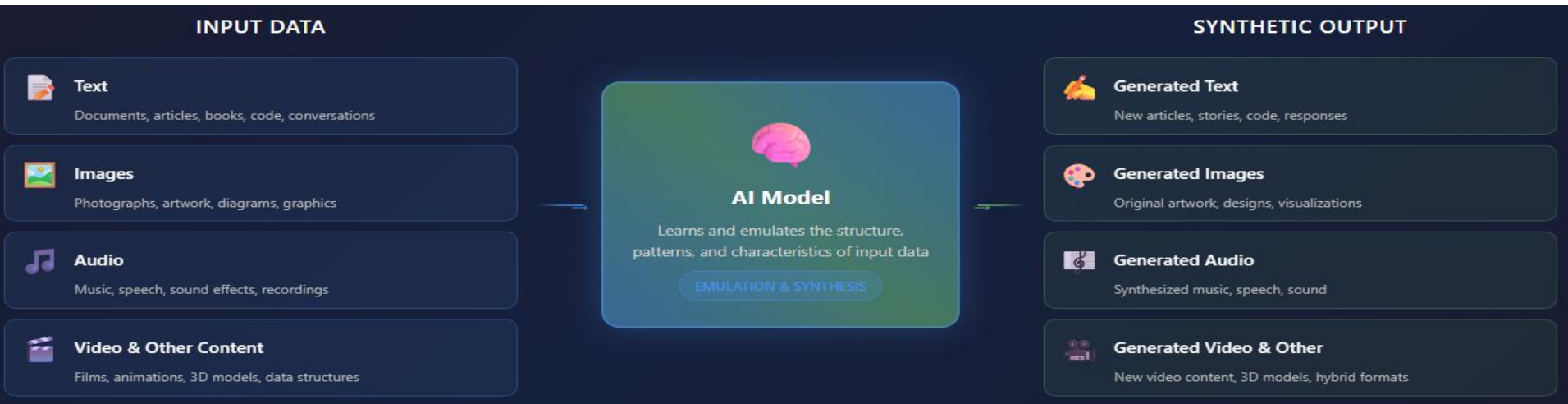
## Time to Reach 100 Million Users



*ChatGPT reached 100M users before most LE agencies knew it existed.*

# What is Gen AI ?

Generative AI systems **learn from vast examples** and develop an **intuition for what comes next**, enabling them to model structure and patterns in input data and **produce entirely new content**.



Source: NIST Glossary of Key Information Security Terms, "Generative Artificial Intelligence (Gen AI)", SP-800-218A

#IACP2026

© Jonathan Lewin, created with Claude AI

# Generative AI: From Data to Predictions

How AI models learn patterns and become advanced prediction engines

1

## Massive Data Input



### Billions of text documents

Books, articles, websites, code, conversations



### Millions of images

Photos, art, diagrams, screenshots



### Diverse knowledge domains

Science, culture, languages, patterns

2

## Pattern Learning Engine



### Self-Teaching Process

- ⚡ Analyzing billions of examples
- 🔍 Discovering hidden patterns
- 🔗 Building neural connections
- 🔧 Optimizing predictions

3

## Intelligent Generation



### Text Prediction

Predicting next words & letters

PREDICTING NEXT WORD:

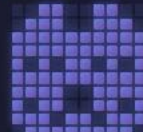
```
Machine learnin|
```



### Image Generation

Predicting pixels & patterns

PREDICTING PIXELS:



### Code Generation

Predicting code patterns

WRITING CODE:

```
model.process(ite|
```



## Advanced Prediction Engine

Through training on massive datasets, the AI learns deep patterns in language, images, and concepts. It becomes a sophisticated prediction engine that can forecast the most likely next word, pixel, or code token—generating coherent images, answering questions, and creating entirely new content by understanding and applying the patterns it discovered during training.

# WHAT AI THINKS AI CAN HELP WITH



*ChatGPT Prompt: "What are examples of public safety uses of AI?"*

Category	Description	Example
Crime Detection	AI analyzes data from various sources to identify potential criminal activity.	<ul style="list-style-type: none"><li>* <b>Surveillance Cameras &amp; Drones:</b> AI detects suspicious behavior or objects in footage.</li><li>* <b>Sensors:</b> Networks of sensors can detect gunshots, hazardous materials, or crowd density.</li></ul>
Crime Prevention	AI helps predict and prevent crime by analyzing patterns and allocating resources.	<ul style="list-style-type: none"><li>* <b>Predictive Policing:</b> AI analyzes historical crime data to pinpoint high-risk areas for patrols.</li><li>* <b>Person-Based Risk Models:</b> AI assesses an individual's risk of committing a crime.</li><li>* <b>Resource Allocation Models:</b> AI optimizes officer deployment based on real-time crime data.</li><li>* <b>Community Policing:</b> AI tools can be used for better communication and trust-building between police and communities.</li></ul>
Crime Investigations	AI expedites and improves the accuracy of investigations.	<ul style="list-style-type: none"><li>* <b>DNA Analysis:</b> AI assists in faster and more accurate DNA analysis of evidence.</li><li>* <b>Facial Matching:</b> AI helps identify suspects through facial recognition in video footage.</li><li>* <b>LPR (License Plate Recognition):</b> AI automates license plate reading for stolen vehicles or missing persons.</li><li>* <b>Forensic Analysis:</b> AI helps analyze complex digital evidence like phone data.</li><li>* <b>Report-Writing:</b> AI helps police officers and detectives write preliminary and follow-up reports leveraging available information.</li></ul>
Management	AI helps optimize police operations and officer well-being.	<ul style="list-style-type: none"><li>* <b>Officer Wellness:</b> AI can monitor officer stress levels and recommend interventions to promote well-being.</li><li>* <b>Training:</b> AI can personalize officer training based on individual strengths and weaknesses.</li></ul>
Accountability	AI promotes transparency and accountability within police forces.	<ul style="list-style-type: none"><li>* <b>Early Intervention Systems:</b> AI analyzes officer body camera footage to identify potential use-of-force incidents.</li></ul>

# AI Model Capabilities Comparison — April 2026

Capability	ChatGPT	Claude	Gemini	Copilot	Grok
Report & Document Writing	✓	★	✓	✓	✓
Coding & Development	✓	★	✓	✓	✓
Reasoning & Analysis	✓	✓	★	✓	✓
Math & Data Analysis	✓	✓	★	✓	✓
Research / Long Context	✓	✓	★	✓	✓
Real-time Web Search	✓	✓	✓	✓	★
Privacy & Safety Design	✓	★	✓	✓	✓
General Use & Ecosystem	★	✓	✓	✓	✓

★ Best in class

✓ Capable

— Not a focus area

Copilot intelligence powered by GPT · ★ based on published benchmark data — see Sources slide

# Sources & Benchmark References

All ★ (Best in Class) designations are based on publicly available benchmark data as of April 2026.

## ★ Coding & Development — Claude leads

SWE-bench Verified Leaderboard: Claude Opus 4.5/4.6 leads real-world GitHub issue resolution (~77–81%). Powers Cursor, Windsurf, and Claude Code. Stack Overflow Developer Survey 2025: 68% of devs cite GitHub Copilot (GPT-powered) as primary AI tool. [swebench.com](https://swebench.com) · [stackoverflow.com/research/developer-survey-2025](https://stackoverflow.com/research/developer-survey-2025)

## ★ Reasoning & Analysis — Gemini leads

LMarena / Chatbot Arena: Gemini 3 Pro first model to break 1,500 Elo — the highest-ever score on the human-preference leaderboard (Mar 2026). ARC-AGI-2 abstract reasoning: Gemini 3 Pro leads among commercial models. [lmarena.ai](https://lmarena.ai) · [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026)

## ★ Math & Data Analysis — Gemini leads

AIME 2025 competition math: Gemini 3 Pro 95.0%, GPT-5.x 94.6–100% (near-parity). Gemini Deep Think mode demonstrates strongest performance on advanced mathematical reasoning tasks. [overchat.ai/ai-hub](https://overchat.ai/ai-hub) (Dec 2025) · [getpassionfruit.com](https://getpassionfruit.com) (Dec 2025)

## ★ Research / Long Context — Gemini leads

Gemini 3 Pro context window: 1,000,000 tokens (≈750,000 words). Enables processing of entire case files, legal documents, or research corpora in a single session. Claude Opus 4.x: 200K tokens; GPT-5: 128K; Grok 4: 256K. [gurusup.com/blog/ai-comparisons](https://gurusup.com/blog/ai-comparisons) (Apr 2026)

## ★ Report & Document Writing — Claude leads

Multiple head-to-head writing evaluations rate Claude as producing 'the most natural prose' and 'most soul in writing.' Claude outputs up to 128K tokens per response — the longest of any model — enabling full-length reports in a single pass. [getpassionfruit.com](https://getpassionfruit.com) (Dec 2025) · [leahware.co](https://leahware.co) (Jan 2026)

## ★ Real-time Web Search — Grok leads

Grok 4 has native real-time access to the X (Twitter) social graph — live posts, trending discussions, breaking news. Unique among the five models. All others offer search integration, but none have this social-intelligence pipeline. [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026) · [gurusup.com](https://gurusup.com) (Apr 2026)

## ★ Privacy & Safety Design — Claude leads

Claude is designed with 'strictest data defaults' among consumer AI tools ([pritamroy.com](https://pritamroy.com)). Anthropic's Constitutional AI approach targets safety-first design. Note: None of these models are CJIS-certified by default — enterprise/cloud deployments require separate review. [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026) · [anthropic.com/privacy](https://anthropic.com/privacy)

## ★ General Use & Ecosystem — ChatGPT leads

ChatGPT is the most widely adopted AI assistant globally. Powers Microsoft Copilot, GitHub Copilot, and thousands of third-party integrations. OpenAI's GPT models are in 85% of Fortune 500 via Microsoft platforms (Microsoft 2025). [intuitionlabs.ai](https://intuitionlabs.ai) (Apr 2026) · [microsoft.com/en-us/ai](https://microsoft.com/en-us/ai)

# AI PANEL DISCUSSION



#IACP2026

# Cinematic panel with mouth animation restored and scripted reactions that trigger automatically at the right moments during dialogue.

● Live AI in law enforcement · panel discussion



ChatGPT  
Panelist

Gemini  
Moderator

Grok  
Panelist

Now Opening 0%

● Gemini · Moderator

Welcome back. I'm Gemini. ChatGPT and Grok are with me. Let's go.

◀ Previous



Next ▶

1 / 17

1.15x ▾

🔄 Restart

# AI Model Capabilities Comparison — April 2026

Capability	ChatGPT	Claude	Gemini	Copilot	Grok
Report & Document Writing	✓	★	✓	✓	✓
Coding & Development	✓	★	✓	✓	✓
Reasoning & Analysis	✓	✓	★	✓	✓
Math & Data Analysis	✓	✓	★	✓	✓
Research / Long Context	✓	✓	★	✓	✓
Real-time Web Search	✓	✓	✓	✓	★
Privacy & Safety Design	✓	★	✓	✓	✓
General Use & Ecosystem	★	✓	✓	✓	✓

★ Best in class

✓ Capable

— Not a focus area

Copilot intelligence powered by GPT · ★ based on published benchmark data — see Sources slide

# Sources & Benchmark References

All ★ (Best in Class) designations are based on publicly available benchmark data as of April 2026.

## ★ Coding & Development — Claude leads

SWE-bench Verified Leaderboard: Claude Opus 4.5/4.6 leads real-world GitHub issue resolution (~77–81%). Powers Cursor, Windsurf, and Claude Code. Stack Overflow Developer Survey 2025: 68% of devs cite GitHub Copilot (GPT-powered) as primary AI tool. [swebench.com](https://swebench.com) · [stackoverflow.com/research/developer-survey-2025](https://stackoverflow.com/research/developer-survey-2025)

## ★ Reasoning & Analysis — Gemini leads

LMarena / Chatbot Arena: Gemini 3 Pro first model to break 1,500 Elo — the highest-ever score on the human-preference leaderboard (Mar 2026). ARC-AGI-2 abstract reasoning: Gemini 3 Pro leads among commercial models. [lmarena.ai](https://lmarena.ai) · [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026)

## ★ Math & Data Analysis — Gemini leads

AIME 2025 competition math: Gemini 3 Pro 95.0%, GPT-5.x 94.6–100% (near-parity). Gemini Deep Think mode demonstrates strongest performance on advanced mathematical reasoning tasks. [overchat.ai/ai-hub](https://overchat.ai/ai-hub) (Dec 2025) · [getpassionfruit.com](https://getpassionfruit.com) (Dec 2025)

## ★ Research / Long Context — Gemini leads

Gemini 3 Pro context window: 1,000,000 tokens (≈750,000 words). Enables processing of entire case files, legal documents, or research corpora in a single session. Claude Opus 4.x: 200K tokens; GPT-5: 128K; Grok 4: 256K. [gurusup.com/blog/ai-comparisons](https://gurusup.com/blog/ai-comparisons) (Apr 2026)

## ★ Report & Document Writing — Claude leads

Multiple head-to-head writing evaluations rate Claude as producing 'the most natural prose' and 'most soul in writing.' Claude outputs up to 128K tokens per response — the longest of any model — enabling full-length reports in a single pass. [getpassionfruit.com](https://getpassionfruit.com) (Dec 2025) · [leahware.co](https://leahware.co) (Jan 2026)

## ★ Real-time Web Search — Grok leads

Grok 4 has native real-time access to the X (Twitter) social graph — live posts, trending discussions, breaking news. Unique among the five models. All others offer search integration, but none have this social-intelligence pipeline. [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026) · [gurusup.com](https://gurusup.com) (Apr 2026)

## ★ Privacy & Safety Design — Claude leads

Claude is designed with 'strictest data defaults' among consumer AI tools ([pritamroy.com](https://pritamroy.com)). Anthropic's Constitutional AI approach targets safety-first design. Note: None of these models are CJIS-certified by default — enterprise/cloud deployments require separate review. [pritamroy.com/blog](https://pritamroy.com/blog) (Mar 2026) · [anthropic.com/privacy](https://anthropic.com/privacy)

## ★ General Use & Ecosystem — ChatGPT leads

ChatGPT is the most widely adopted AI assistant globally. Powers Microsoft Copilot, GitHub Copilot, and thousands of third-party integrations. OpenAI's GPT models are in 85% of Fortune 500 via Microsoft platforms (Microsoft 2025). [intuitionlabs.ai](https://intuitionlabs.ai) (Apr 2026) · [microsoft.com/en-us/ai](https://microsoft.com/en-us/ai)



Grok

Gemini

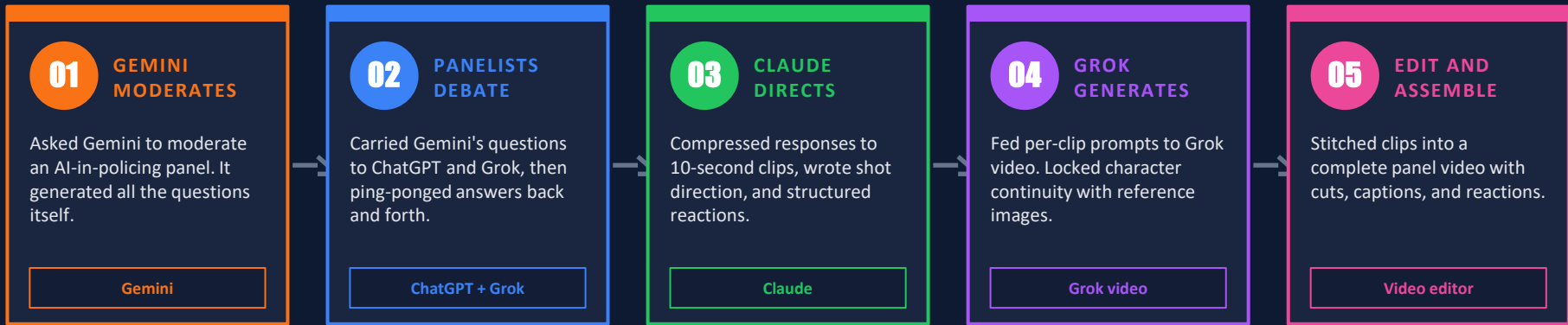
ChatGPT



# HOW THIS AI PANEL WAS BUILT



Five AI tools, one workflow — no studio, no production crew



## WHAT MADE IT WORK

Each model played to its strength. Gemini moderated and crafted questions unprompted. ChatGPT argued process and legitimacy. Grok argued speed and outcomes. Claude wrote and directed.

## WHAT THE AUDIENCE SEES

A polished broadcast-style panel of three named AI characters debating real policing tradeoffs — bias, transparency, public trust — with reactions, cutaways, and TV-news styling.

## WHY THIS MATTERS FOR LE

A workshop demo that would have cost thousands and taken weeks now takes one person, one afternoon, and zero programming. The barrier to AI-assisted content creation has collapsed.

# Two Paths for AI-Assisted Analysis

Crime analysis, workload review, early intervention — the right path depends on your data's sensitivity

STEP 1 **Find the data** · Determine its sensitivity → *public open data, internal RMS / CAD, OSINT, multiple sources for correlation*

## PATH A · CLOUD LLM

*Public, aggregated, or sanitized data*

### Direct to a hosted AI model

1. Confirm data is safe to share
2. Prompt Claude / ChatGPT / Gemini
3. Get analysis, maps, reports, Q&A, correlations

**JUST DEMOED** Fort Worth crime briefing ←

## PATH B · VIBE-CODED LOCAL

*Internal records, PII, CJIS-sensitive*

### AI writes the tool, you run it locally

1. Build a cleaned sample to model the schema
2. Prompt Claude to vibe-code the analysis tool
3. Run locally — full sensitive data never leaves your network

**UP NEXT** Intervention Simulator + Crime Mapping Dashboard →

ALSO FOR SENSITIVE DATA — TWO ALTERNATIVES TO LOCAL VIBE-CODING

### CJIS-CLEARED ENTERPRISE CLOUD

#### Hosted LLM, but in a CJIS-compliant boundary

AWS Bedrock GovCloud · Azure GovCloud (O365) · Palantir AIP gateway — procurement + agency security review required

### AIRGAPPED LOCAL LLM

#### Run the model itself on agency hardware

Open-source models (Llama, Mistral, etc.) on internal servers — no cloud, no internet, total data control; requires GPU infrastructure

# Generate Your Own Crime Analysis Report

Four steps from raw incident data to a command-ready PDF briefing — no programming required

## 1 FIND THE DATA

### Source the dataset

- City / county open data
- FBI Crime Data Explorer
- State UCR / NIBRS feeds
- Internal RMS or CAD export

CSV · EXCEL · JSON

## 2 STRIP PII / CJIS

### Sanitize the data first

- Remove names, DOBs, SSNs
- Redact juvenile identifiers
- Confirm no DV / SA detail
- Aggregate to block level

CRITICAL FOR LE DATA

## 3 UPLOAD TO CLAUDE

### Drop the file in chat

- Fresh chat, fresh context
- Files up to ~250 MB
- CSV preferred for large sets
- One file, one chat

ONE FILE · ONE CHAT

## 4 PROMPT

### Paste the template

- Claude inspects the schema
- Classifies offenses (NIBRS)
- Adapts to data on hand
- Produces the PDF briefing

OUTPUT IN MINUTES

### WHAT YOU GET BACK

12–16 page command briefing → Executive summary with KPIs → Trend analysis → Hotspot maps → Violent / property deep-dives → Findings & methodology

# CRIME ANALYSIS BRIEFING

## Comprehensive Trend & Pattern Snapshot

Reported Incidents | January 2005 – September 2021

Source: City Open Data — Police Crime Data Table

Records analyzed: 1,156,979

Audience: City Leadership

Classification: Aggregate, non-attributed

### KEY FINDINGS AT A GLANCE

#### MAJOR FINDINGS

- **Scale:** 1,156,979 incidents analyzed across 16.75 years (Jan 2005 – Sept 2021), spanning 58 NIBRS offense codes and 86,178 unique block addresses.
- **Composition:** 57.6% property, 29.2% society/order, 13.3% violent. Vehicle-related crime alone (theft-from-MV + MV theft + parts) exceeds 183,000 incidents — larger than the entire violent crime category.
- **Spatial concentration:** 3.9% of blocks produce 50% of crime; 16.3% produce 80%. The top 15 addresses alone account for 3.7% of citywide volume.

#### TRENDS

- **Long-term direction:** Overall reported volume down ~32% from 2008 peak (88k → 58k by 2020). Property crime drove virtually all of that decline.
- **Recent bifurcation:** 2018–2021 broke the pattern: property kept falling while violent crime turned upward. Homicides surged 2.7× — from a stable ~32/year baseline to 86 in 2020 — mirroring the national pandemic-era pattern.

#### CORRELATIONS

- **Temporal:** Violent crime concentrates Friday–Saturday 8 PM through 3 AM Sunday; property crime is the opposite — weekday afternoon peaking 5–6 PM. Summer months run ~10% above winter.
- **Locational:** Top-volume blocks are commercial corridors and arterials (opportunity-driven). Violent-specific hotspots diverge — Las Vegas Trail, E Lancaster, Cypress St emerge as distinct concentrations not captured by all-crime rankings.

#### PROJECTIONS

- **Linear extrapolation:** Long-term trend implies ~1,200 fewer incidents per year; recent-period slope (2016–2020) is steeper at ~1,600/yr — but this aggregate masks the property-down / violent-up split.
- **Critical caveat:** Data ends September 2021 — pre-pandemic-normalization. Treat this report as the historical baseline; pair with a refreshed 2022–2025 extract to determine which 2018–2021 movements were transient versus structural.

### Executive Summary

TOTAL INCIDENTS

1.16M

2005 – Sept 2021 (16.75 yrs)

VIOLENT CRIME

153,304

13.3% of all incidents

PROPERTY CRIME

666,248

57.6% of all incidents

HOMICIDES

670

17-year total; 2020 peak: 86

This report consolidates 1,156,979 reported incidents spanning January 2005 through September 2021 — approximately 16.75 years of police crime data published through the City's Open Data portal. The dataset captures over a million events across 58 distinct NIBRS offense codes at 86,178 unique block addresses, geolocated for 60,000+ incidents.

The long-term direction is favorable. Annual reported volume declined from 84,561 incidents in 2006 (first full year of reporting) to 57,888 in 2020 — a 32% decrease over 14 years. However, the final two years showed a meaningful divergence: violent crime — and specifically homicides — surged sharply in 2019–2020, mirroring the national pandemic-era pattern.

#### What's up

- Homicides ↑ 145% 2018 → 2020 (25 → 86) — a 17-year high
- Aggravated assault ↑ sharply from 2018 onward
- Weapons violations ↑ after 2018
- Motor Vehicle Theft ↑ in 2020 after years of decline

#### What's down

- Burglary ↓ ~62% (peak ~9,400 in 2008 → 3,500 by 2020)
- Property crime overall ↓ 36% 2008 → 2020
- Theft / Larceny ↓ steadily across the period
- Robbery ↓ ~35% from 2009 peak

#### Where crime concentrates

- 3,395 blocks (3.9%) produce 50% of all crime
- 14,063 blocks (16.3%) produce 80% of all crime
- Peak hour: 6 PM overall; Sat–Sun 00:00–02:00 for violent
- Top venue type: Residence/Home (40% of incidents)

**Data caveats:** (1) The dataset effectively ends in September 2021; no representative 2022–2025 data is included. Trends after Sept 2021 must be sourced separately. (2) Sex offenses (NIBRS 11A–D) are essentially absent from this public extract — standard open-data privacy suppression. (3) Geographic Beat / Division / Council District fields are only populated from 2019 onward; division-level comparisons before 2019 are unsupported. (4) The 00:00 hour cell in temporal heatmaps is inflated by data-entry default when occurrence time is unknown.

## 1. Overall Trend & Category Mix

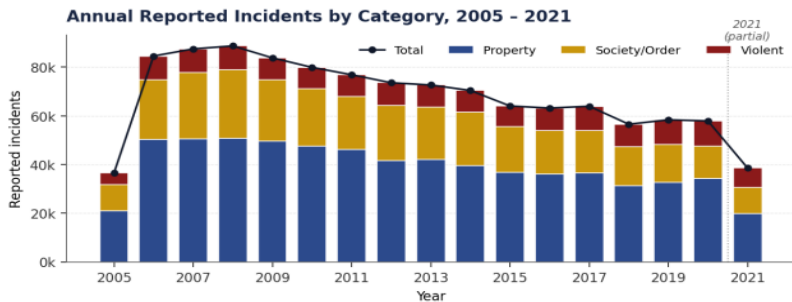


Figure 1.1 — Annual reported incidents, stacked by category. 2005 is a partial onboarding year; 2021 is partial (Jan–Sept). The black line is the total.

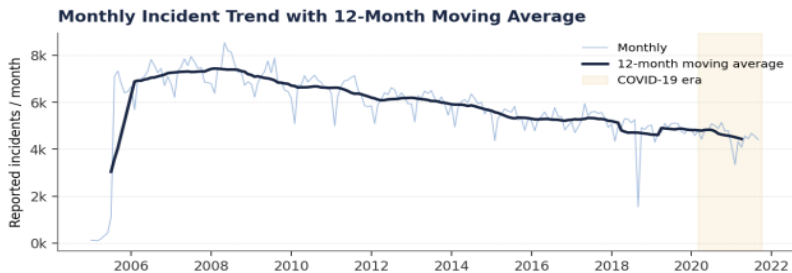


Figure 1.2 — Monthly counts (light blue) with a 12-month moving average (dark navy) to smooth out seasonality and isolate the underlying trend. The shaded band marks the COVID-19 era.

### Three eras stand out in the 17-year record:

- **2006 – 2008 — High plateau:** Annual volume peaked at **88,720 (2008)** and stayed above 83,000 for three consecutive years. Property crime dominated the mix.
- **2009 – 2017 — Sustained decline:** Crime fell almost monotonically year over year, reaching the mid-60,000s. Property crime drove most of the reduction; violent crime was flat to modestly declining.
- **2018 – 2021 — Bifurcation:** Property crime continued to ease, but violent crime and especially homicides moved sharply higher. The pandemic accelerated this divergence.

## 2. Primary Crime Types

Over the 16.75-year period, the **top 15 offense types account for roughly 87%** of all reported incidents. The list is dominated by property and order offenses; the highest-volume violent crime (simple assault) ranks sixth overall.

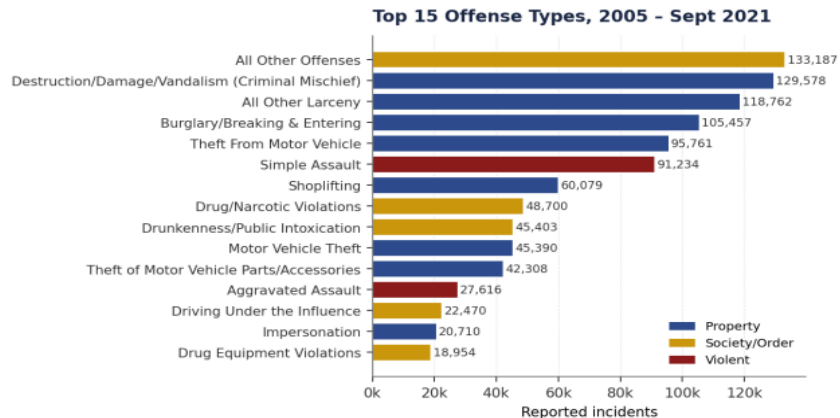


Figure 2.1 — Top 15 offense types, color-coded by category. Three offenses each exceed 100,000 incidents: criminal mischief / vandalism, burglary of vehicle, and "all other larceny."

### Key offense observations

- **Vehicle-related crime is enormous:** If we combine theft from motor vehicle (96k), motor vehicle theft (45k), and theft of MV parts/accessories (42k), **vehicle crime alone exceeds 183,000 incidents** — more than the entire violent crime category.
- **Larceny is the single largest crime family:** All theft / larceny subcategories combined (NIBRS 23A–23H) total over 323,000 incidents — 28% of all crime.
- **Burglary is the third-largest category** at 105,000+ incidents across the period.
- **Criminal mischief / vandalism is #1 by volume** at 129,000+ incidents — a high-cost "quality of life" crime that often signals neighborhood disorder.
- **Among violent offenses**, simple assault (91k) is roughly 3× the volume of aggravated assault (28k), which is roughly 1.7× the volume of robbery (16k).

### 3. When — Temporal Patterns

Temporal patterns reveal where police staffing and prevention effort yield the highest return. The Fort Worth data shows pronounced day-of-week, hour-of-day, and seasonal concentration — patterns that have remained remarkably stable across the 17-year window.

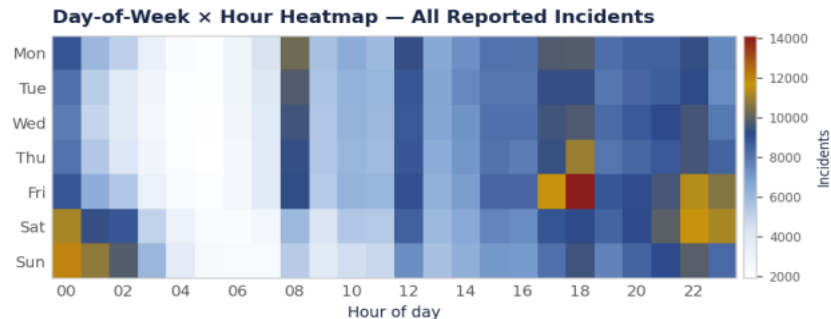


Figure 3.1 — Day-of-week x hour heatmap for all reported incidents. Darker / hotter cells indicate more incidents. The 00:00 column is partly inflated by data-entry default behavior when the precise occurrence time is unknown.

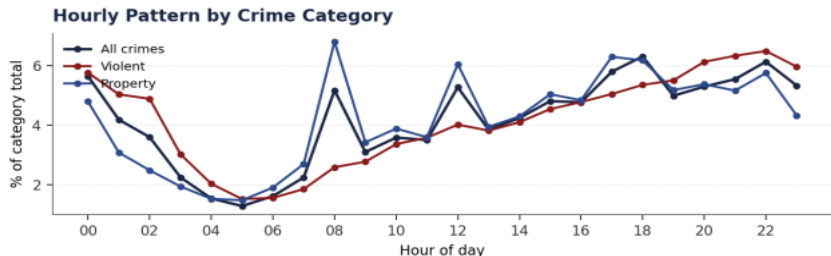


Figure 3.2 — Hourly distribution shown as percentage of each category total. Note the divergence: property crime peaks during daytime / evening commercial hours, while violent crime concentrates after dark, with a secondary peak in the late evening.

### 4. Where — Geographic Concentration

Crime in Fort Worth follows a textbook “Power Few” pattern: a small set of locations generate a disproportionate share of incidents. This is the single most actionable finding in the report — it tells leadership where focused intervention will produce the largest return on effort.

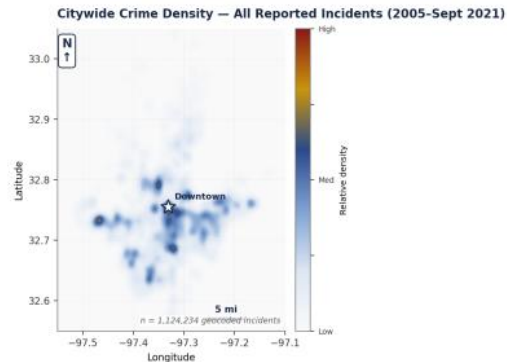


Figure 4.1 — Citywide kernel density of all reported incidents 2005–Sept 2021 (n=1.12M geocoded). Distinct concentrations are visible in central Fort Worth, east of downtown along the Lancaster corridor, and a notable cluster in west Fort Worth.

### Spatial Concentration of Crime — Pareto / 80-20 Analysis

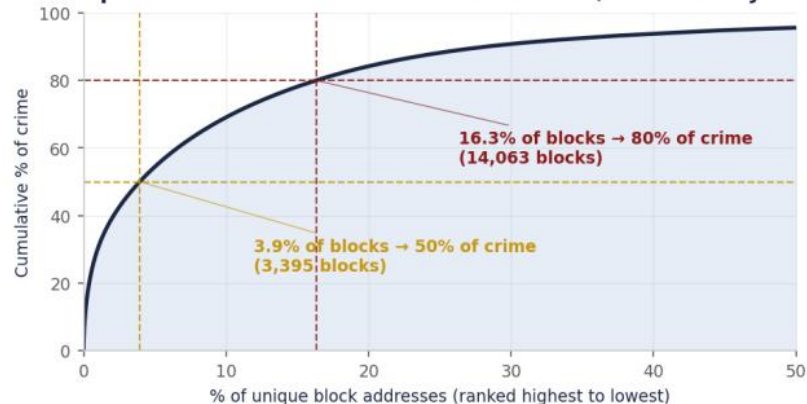


Figure 4.2 — Pareto / 80-20 analysis. Cumulative share of crime (y-axis) plotted against the cumulative share of unique block addresses (x-axis), ranked highest to lowest. The sharp curvature confirms strong spatial concentration: just 3.9% of all blocks produce 50% of crime, and 16.3% of blocks produce 80%.

**SAMPLE OUTPUT** Below: actual pages from a 15-page briefing produced from a 1.16M-record municipal crime dataset



**What's inside** → Cover with at-a-glance bullets (Major Findings / Trends / Correlations / Projections) • Executive summary with KPI cards • Annual & monthly trends + 12-month moving average • Top crime types color-coded by category • DOW+Hour heatmaps • Geographic concentration (KDE hotspot maps, Pareto 80/20 curve, top blocks) • Violent & property deep-dives • Linear projection with caveat • Findings, methodology, & stated limitations

**THE PROMPT** Paste into a new Claude chat with your dataset attached. Claude inspects the data, adapts the analysis to what's available, and produces the PDF.

```

You are a senior crime analyst. I'll attach a crime/incident dataset (CSV, Excel, or similar). Produce a polished PDF briefing ('Crime_Analysis_Briefing.pdf') suitable for command staff, elected officials, or community stakeholders - 12-16 pages, plain language, strong visuals, defensible numbers.

# CORE PRINCIPLE
Don't assume the schema. Inspect the data first, figure out what's actually there, and shape the analysis around what the data supports. Don't ask clarifying questions unless the file is unreadable - proceed, make reasonable choices, document them in the report.

# STEP 1 - DATA DISCOVERY (before any chart code)
Lead a sample and report briefly:
- File shape, rows, column names, dtypes
- For each column: % populated, sample values, apparent meaning
- Identify the analytical fields: date/time, offense/crime-type, location, premise type, anything else useful.
- Effective date range; flag if recent months are partial/stale
- Obvious gaps or suppression (e.g., sex offenses missing)
Continue even if some fields are missing. Surface caveats in the report.

# STEP 2 - CRIME CLASSIFICATION (adapt to data)
Group offenses into three FBI/NIBRS-aligned buckets:
- VIOLENCE: homicide, assault, robbery, intimidation, kidnapping, human trafficking, sex offenses if present
- PROPERTY: burglary, larceny/theft, MOT, theft from MV, vandalism, arson, fraud, forgery, embezzlement, stolen property
- SOCIETY/ORDER: drug & narcotic, DUI/DWI, weapons, prostitution, disorderly conduct, trespass, liquor, gambling, warrants
If NIBRS/UCR codes → use the official taxonomy. If only free-text → keyword classifier covering 295% of records. If only call-types → group by best judgment and disclose mapping. Show logic in methodology.

# STEP 3 - LOCATION HANDLING (whatever data supports)
Geographic analysis tier - use the highest the data supports:
TIER 1: lat/lon → KDE hotspot maps + scatter density
TIER 2: addresses → geocode sample via Nominatin/OSM
TIER 3: addresses only, no geocoding → block-level concentration, Pareto curve, beat/district aggregation, top-20 block bar chart
TIER 4: no location → drop geo sections, expand temporal/offense
Always do block-level Pareto (city location string exists).

# STEP 4 - REQUIRED ANALYSES (skip cleanly if unsupported)
1. Annual trend stacked by category + monthly 12-mo moving average; band any obvious era (COVID, policy change)
2. Top 15 offense types color-coded by category
3. Category composition donut + plain-English bucket explanation
4. Temporal (if time-of-day exists): DOW*Hour heatmap, hour-curve comparing violent vs property, DOW bars, monthly seasonality

5. Geographic concentration - scale to tier from Step 3
6. Top blocks + premise/location/type breakdown (if present)
7. Violent deep-dive: KPI cards, stacked yearly composition, homicide per year, robbery vs assault vs violent timing & geography
8. Property deep-dive: KPIs, yearly composition, burglary/MOT/theft trend lines, property timing
9. Projection: linear fit (all-year + recent-5yr slope, directional indicator only - call out aggregate vs category-level divergence
If a metric's data is unavailable, note what would be needed.

# STEP 5 - VISUAL STYLE
Command-briefing palette: Navy #1a2744, Gold #c9950c, Red #8b1a1a (violent), Blue #004a8c (property). Clean sans-serif, minimal spines, no chart junk. Legends OUTSIDE plot area on stacked charts. Donut & labels OUTSIDE wedges. Annotations in clean whitespace, never on top of dashed reference lines. KDE colormap: white-to-blue-to-gold-to-red. Letter size, <0.5" side margins, <0.85" top margin.

# STEP 6 - PDF STRUCTURE
1. COVER - heavy header, title, KEY FINDINGS AT A GLANCE with gold underline; bullets grouped MAJOR FINDINGS / TRENDS / CORRELATIONS / PROJECTIONS
2. Executive Summary - 4 KPI cards, narrative, What's up / What's down / Where it concentrates columns, data caveats callout
3. Overall Trend & Category Mix
   - Primary Crime Types
4. Temporal Patterns (omit if no time-of-day)
5. Geographic Concentration (scale to Tier from Step 3)
6. Violent Crime Deep-Dive
7. Violent Timing & Geography
10. Property Crime Deep-Dive
11. Trend Lines & Forward Look
12. Findings & Methodology + Stated Limitations
Use ReportLab 'KeepTogether' to bind charts with captions and headers with content. Consolidate aggressively - no orphan captions.

# STEP 7 - QUALITY BAND (before delivery)
- Band on every page to top and bottom
- Check legend/overlapping-bars, axis/vtick collisions, orphaned captions, donut labels obscuring central text, off-page elements
- If a page is mostly whitespace, check prior chart or consolidate
- Aim for 516 pages total

# OUTPUT
Save: '/mnt/user-data/outputs/Crime_Analysis_Briefing.pdf'. Then give a one-sentence summary of what you produced, what choices you made (e.g., 'no coordinates due to Tier 3 block-level concentration'), and what's NOT included due to data limitations.
Begin by inspecting the file.

```

**MODIFICATIONS** Append any of these to the prompt above to customize for your situation

- Small dataset (<10k records). Don't attempt KDE smoothing or projections - sample size insufficient. Show raw counts and percentages only.
- Campus / single-precinct data. Frame as operational rather than citywide - reference deployment, patrol, prevention rather than 'city leadership.'
- Specific audience. Target audience is [city council / sheriff / community advisory board] - adjusts tone and what counts as actionable.
- Different output format. "Output as an interactive HTML dashboard" OR "Output as a PowerPoint deck with one chart per slide."
- Custom branding. "Use [agency name] on the cover; replace navy/gold palette with [your colors]."
- Add comparison context. "Where possible, contextualize trends against state / FBI national rates for the same offense categories."

You are a senior crime analyst. I'll attach a crime/incident dataset (CSV, Excel, or similar). Produce a polished PDF briefing ('Crime\_Analysis\_Briefing.pdf') suitable for command staff, elected officials, or community stakeholders - 12-16 pages, plain language, strong visuals, defensible numbers.

## # CORE PRINCIPLE

Don't assume the schema. Inspect the data first, figure out what's actually there, and shape the analysis around what the data supports. Don't ask clarifying questions unless the file is unreadable - proceed, make reasonable choices, document them in the report.

## # STEP 1 - DATA DISCOVERY (before any chart code)

Lead a sample and report briefly:

- File shape, rows, column names, dtypes
  - For each column: % populated, sample values, apparent meaning
  - Identify the analytical fields: date/time, offense/crime-type, location, premise type, anything else useful
  - Effective date range; flag if recent months are partial/stale
  - Obvious gaps or suppression (e.g., sex offenses missing)
- Continue even if some fields are missing. Surface caveats in the report.

## # STEP 2 - CRIME CLASSIFICATION (adapt to data)

Group offenses into three FBI/NIBRS-aligned buckets:

- VIOLENCE: homicide, assault, robbery, intimidation, kidnapping, human trafficking, sex offenses if present
  - PROPERTY: burglary, larceny/theft, MV/T, theft from MV, vandalism, arson, fraud, forgery, embezzlement, stolen property
  - SOCIETY/ORDER: drug & narcotic, DUI/DWI, weapons, prostitution, disorderly conduct, trespass, liquor, gambling, warrants
- If NIBRS/UCR codes → use the official taxonomy. If only free-text → keyword classifier covering 295% of records. If only call-types → group by best judgment and disclose mapping. Show logic in methodology.

## # STEP 3 - LOCATION HANDLING (whatever data supports)

Geographic analysis tier - use the highest the data supports:

- TIER 1: lat/lon → KDE hotspot maps + scatter density
  - TIER 2: addresses → geocode sample via Nominatin/OSM
  - TIER 3: addresses only, no geocoding → block-level concentration, Pareto curve, beat/district aggregation, top-20 block bar chart
  - TIER 4: no location → drop geo section; expand temporal/offense
- Always do block-level Pareto if any location string exists.

## # STEP 4 - REQUIRED ANALYSES (skip cleanly if unsupported)

- Annual trend stacked by category + monthly 12-mo moving average; band any obvious era (COVID, policy change)
- Top 15 offense types color-coded by category
- Category composition donut + plain-English bucket explanation
- Temporal (if time-of-day exists): DOW\*Hour heatmap, hour-curve comparing violent vs property, DOW bars, monthly seasonality

# App Development Examples



Building Real Tools Through AI Collaboration

## DESCRIBE

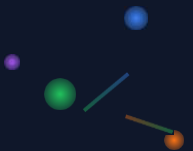
Tell Claude what you want to build

## BUILD

AI generates working code

## DEPLOY

Run locally or in the cloud



# Two Quick App Demos

Building real tools through conversation — no programming required

## 1 INTERVENTION SIMULATOR

Simulate impact of crime intervention strategies on a Chicago police district

Research-backed interventions

Interactive sliders for impact testing

Generates implementation plans

Cites peer-reviewed sources

West Garfield Park, 11th District

## 2 CRIME MAPPING DASHBOARD

Create a working crime mapping dashboard for a Chicago police district

Live data from public API

Interactive filtering and analysis

Risk prediction zones

Deployable locally or cloud

19th District Demo

THE APPROACH IS THE SAME

Describe what you want → Identify research/data → Prompt Claude to build → Test and refine → Validate outputs → Deploy

1

# Initial Prompt

Intervention Simulator — Describing the vision in plain language

JL

i want to develop an interactive automated "dashboard" that can test various police intervention strategies on a community and show the impact on crime there, informed by specific actionable research. in other words, i want to translate "research into action," find a few academic papers that would support this, for a chicago neighborhood. we will then model that neighborhood (West side of Chicago, 11th police district, Garfield Park) with real demographics and crime data and measure impacts

GOAL

Interactive dashboard

METHOD

Research-backed interventions

CONTEXT

Real neighborhood data

OUTPUT

Measure impacts

# 1 Modifications

Iterative refinement through conversation

JL It should all fit on one "screen" -- also the interventions should be sliders to see "how much" of the intervention has "how much" impact, also add staffing and add community enhancements like more food stores, less liquor stores, street lighting...

JL Now add an "implement" button that will give me a written proposal outlining the specific interventions, citing specific research showing why they would work, timeline/project plan, and cost - suitable for sending to a city mayor and funding provider for approval.

JL You generated this code from various prompts I provided. However I checked the academic sources you cited and found some issues. I love the app and idea but I need validated verified academic sources. Can you re-work all of this and use verified sources this time? **KEY STEP**

JL Ok now here is a challenge for you. I want to be able to completely re-create this with a brand new prompt of a paragraph or so, in a new session, including these features, the body of research, etc -- what paragraph can do that? And can we test it?

Always verify AI-generated citations and research — Claude can hallucinate sources. Ask it to re-verify!

# 1 After Asking Claude to Verify

Evidence-based interventions with peer-reviewed citations

## VERIFIED PEER-REVIEWED SOURCES

### 1. HOT SPOTS POLICING — 16% reduction

Braga et al. (2019). Campbell review of 65 studies. Journal of Experimental Criminology

### 2. FOCUSED DETERRENCE — 25% reduction (gang violence)

Braga and Weisburd (2018). Campbell review of 24 evaluations. Criminology and Public Policy

### 3. PROBLEM-ORIENTED POLICING — 20% reduction

Hinkle et al. (2020). Campbell review of 34 studies. Campbell Systematic Reviews

### 4. STREET LIGHTING — 14% reduction

Welsh and Farrington (2022). Campbell review of 21 studies. Criminology and Public Policy

### 5. VACANT LOT REMEDIATION — 6.8-9.2% reduction in shootings

Moyer et al. (2019). Philadelphia RCT of 541 lots. American Journal of Public Health

### 6. ALCOHOL OUTLET REDUCTION — Small to moderate effects

Campbell et al. (2009). CDC systematic review. American Journal of Preventive Medicine

## ALSO IDENTIFIED: COST ERROR

Original model used:

**\$587 per crime (too low)**

Actual societal costs:

Murder: \$8.98M

Rape: \$241K

Assault: \$107K

Robbery: \$42K

Source: McCollister et al., 2010

## RECOMMENDATION

Use \$5K-\$15K per crime (weighted average) for realistic positive ROI calculations.

Verify sources. Claude will correct itself when asked!



Your plan ends in 28 days - [Resubscribe](#)

Good afternoon, Jonathan

How can I help you today?



Sonnet 4.5  

-  Write
-  Learn
-  </> Code
-  Life stuff
-  Claude's choice

Want to build from  
your imagination?



## West Garfield Park Crime Intervention Dashboard

✓ VERIFIED RESEARCH SOURCES

Police District 11 | Population: 10,902 | Baseline: 507 crimes/year

Crime Reduction **0.0%**

Crimes Prevented **0**

Officers Needed **0.0**

ROI **0.0%**

Generate Evidence-Based Implementation Proposal

### Community Impact Visualization

Safety Score **0.0%**

Street Lighting **62.0%**

Blight Reduction **0.0%**

Community Trust **38.0%**

Victims Prevented **0**

Economic Benefit **\$0**

### Crime Rate Comparison

Category	Baseline	With Intervention
Violent	~80	~80
Property	~440	~440

Baseline Total **507 crimes/year**

Projected Total **507 crimes/year**

Reduction **0 crimes prevented**

### Intervention Controls

✓ ALL SOURCES VERIFIED

#### POLICING STRATEGIES

Hot Spots Policing **0%**  
Braga et al. (2019): Small but significant effect

Focused Deterrence **0%**  
Braga & Weisburd (2018): Moderate effect for gang violence

Problem-Oriented Policing **0%**  
Hinkle et al. (2020): Modest but significant effect

#### ENVIRONMENTAL INTERVENTIONS

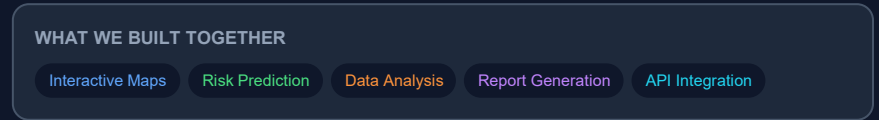
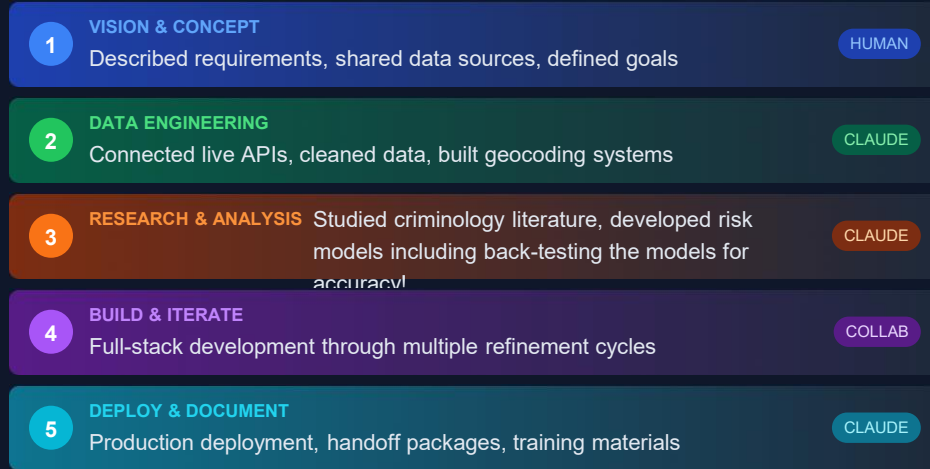
Street Lighting **0%**  
Welsh & Farrington (2022): 14% reduction in overall crime

Vacant Lot Remediation **0%**  
Branas et al. (2018): 6.8-9.2% reduction in shootings

Alcohol Outlet Reduction **0%**  
Campbell et al. (2009): Small to moderate effects on violence

# Crime Mapping Dashboard Project: An AI Collaboration

From concept to deployment — Claude served as assistant, researcher, developer, and collaborator



*If you can dream it, we can build it.*

Claude and I collaborated on this slide too!

# Chicago 19th District Dashboard Demo

7,550 TOTAL +13%
0 PUB VIOLENCE
0 THEFT
0 BATTERY
0 ROBBERY
0% ARRESTS
vs. same period last year

Crime Types: Homicide Robbery Assault Battery Burglary Theft MVT Damage
 Clusters: Has PV No PV
 Time: All 6a-12p 12p-6p 6p-10p 10p-6a
 Day: All M-F S-S
 Search block: 
Export Reset

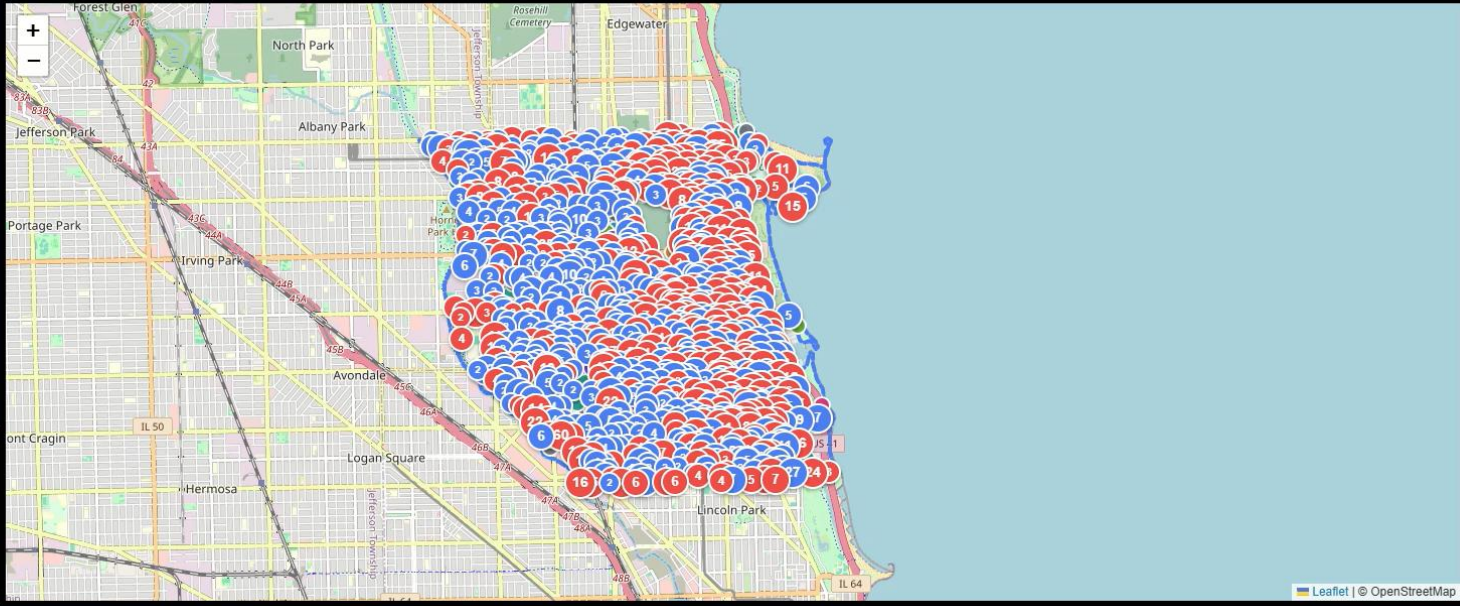
**DATE RANGE**  
 YTD 30d 90d 1yr  
 Start: 06/01/2025 End: 12/31/2025  
 Crime Type: All Crimes  
Load Data

**Analysis Tools**  
Risk Analysis  
Help

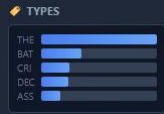
**MAP LAYERS**  
 Boundary  Points  
 Ellipses  Businesses

**Top Hotspots**  
Blocks Zones Risk

1	044XX N BROADWAY	157
2	035XX N CLARK ST	124
3	032XX N CLARK ST	114



**SUMMARY**  
 Date Range: 06-01 to 12-31  
 Total Crimes: 7,550  
 Public Violence: 1262 (17%)  
 Daily Avg: 35.4/day



**Crimes in View**

Date/Time	Type	Description	Block	Location	Beat	Case #	Arrest
2025-12-31 00:00	THEFT	FROM BUILDING	045XX N HAZEL ST	APARTMENT	1914	JK118209	No
2025-12-30 23:45	THEFT	RETAIL THEFT	040XX N LINCOLN AVE	DEPARTMENT STORE	1911	JJ539722	No
2025-12-30 22:30	THEFT	\$500 AND UNDER	047XX N SHERIDAN RD	APARTMENT	1914	JJ539825	No
2025-12-30 22:00	DECEPTIVE PRACTICE	FINANCIAL IDENTITY THEFT OVER	005XX W ARLINGTON PL	nan	1935	JK104572	No

# Getting Started: Two Paths to Build Your Cool New Application

Choose your approach based on data sensitivity and deployment needs

## Cloud Path: Quick Prototyping

For non-sensitive or public data

- 1 Describe Your Vision**  
Tell Claude what you want to build, share sample data
- 2 Claude Builds & Iterates**  
AI creates code, connects APIs, refines based on feedback
- 3 Test in Browser**  
Preview artifacts directly in Claude interface
- 4 Deploy to Cloud**  
PythonAnywhere, Render, or download files to share

Best for: Public data, demos, rapid prototyping. Do not use for CJIS-sensitive data.

## Local Path: CJIS-Secure Deployment

For sensitive law enforcement data: NOTE- Confirm CJIS compliance before using this approach!

- 1 Install Python Locally**  
Download from [python.org](https://python.org), install on secure workstation
- 2 Claude Generates Code**  
Describe needs without sharing sensitive data
- 3 Download & Configure**  
Transfer code to secure environment, add local data
- 4 Run Locally**  
`python server.py` — access at `localhost:5000`

Best for: CJIS data, CAD/RMS, sensitive records. Follow CJIS guidelines for sensitive data.

### RESOURCES

Claude Docs: [docs.anthropic.com](https://docs.anthropic.com) Python: [python.org/downloads](https://python.org/downloads) Flask: [flask.palletsprojects.com](https://flask.palletsprojects.com) Leaflet Maps: [leafletjs.com](https://leafletjs.com)

# Building Apps with AI: The Iterative Process

No coding experience required — just clear communication and iteration

1

## DESCRIBE YOUR VISION

Tell Claude what you want to build in plain language

2

## CLAUDE BUILDS IT

AI generates working code and previews it instantly

3

## TEST AND REFINE

Review results, request changes, iterate until satisfied

4

## EXPORT AND DEPLOY

Download files, publish to GitHub, or run locally

## KEY POINTS

Conversation is your programming language

Each iteration improves the result

Save prompts to recreate apps later

Claude explains what it built and why

## RESOURCES

[claude.ai](https://claude.ai)

Claude Opus 4.5 (paid subscription)

[github.com](https://github.com)

Free hosting for web apps

[docs.anthropic.com](https://docs.anthropic.com)

Official Claude documentation

# Working with Legacy Data in Secure Environments

Use AI to build tools that connect to legacy RMS, CAD, and other systems — without exposing sensitive data. Confirm CJIS compliance for local environment.

1

## GENERATE SAMPLE DATA

Export sample output from your legacy system (RMS, CAD, etc.)

2

## SCRUB SENSITIVE INFO

Remove CJIS data (names, DOBs, etc.) but keep structure intact (do this manually)

3

## CLAUDE ANALYZES STRUCTURE

AI examines format and creates an ingestion strategy

4

## BUILD THE APPLICATION

Claude generates code to parse, process, and visualize data

5

## DEPLOY LOCALLY

Install Python, download code, run on CJIS-secure workstation (confirm CJIS compliance)

6

## CONNECT REAL DATA

Point app at actual legacy systems — even join multiple sources

## WHY THIS WORKS

Sensitive data never leaves your network

Claude only sees sanitized samples

Final app runs 100% locally (ensure CJIS requirements are met)

Bridge data from multiple legacy systems

## RESOURCES

[python.org/downloads](https://python.org/downloads)

Install Python on secure workstation

[flask.palletsprojects.com](https://flask.palletsprojects.com)

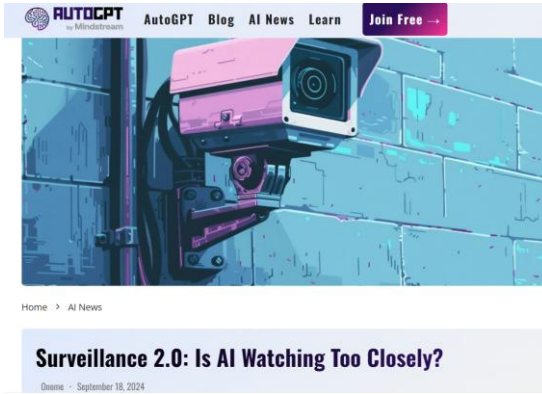
Lightweight web framework

[claude.ai](https://claude.ai)

Claude Opus 4.5 for code generation

All processing happens locally on your CJIS-compliant infrastructure

# And a Warning !!!!



**AUTOGPT** by Mindstream | AutoGPT | Blog | AI News | Learn | [Join Free](#)

## Surveillance 2.0: Is AI Watching Too Closely?

Home > AI News

Channe · September 18, 2024

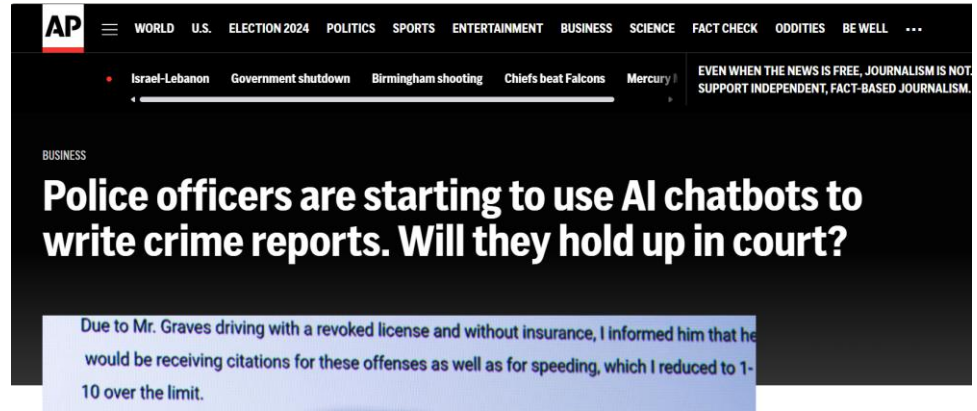
Tech Pulse

## AI is set to revolutionize policing: Are we ready?

Surveillance towers, real-time digital fingerprinting and autonomous patrol cars are just a few examples of the tech-driven revolution in law enforcement

March 04, 2024 05:31 PM • Paul Goldenberg, Michael Gips

#IACP2026



**AP** | WORLD | U.S. | ELECTION 2024 | POLITICS | SPORTS | ENTERTAINMENT | BUSINESS | SCIENCE | FACT CHECK | ODDITIES | BE WELL | ...

Israel-Lebanon | Government shutdown | Birmingham shooting | Chiefs beat Falcons | Mercury | **EVEN WHEN THE NEWS IS FREE, JOURNALISM IS NOT SUPPORT INDEPENDENT, FACT-BASED JOURNALISM.**

BUSINESS

## Police officers are starting to use AI chatbots to write crime reports. Will they hold up in court?

Due to Mr. Graves driving with a revoked license and without insurance, I informed him that he would be receiving citations for these offenses as well as for speeding, which I reduced to 1-10 over the limit.

## LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws



**Johana Bhuiyan**  
Mon 8 Nov 2023 01:00 EST

[Share](#)

**LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws**

POWICE

# The Confidence Paradox



## AI doesn't know what it doesn't know.

It sounds authoritative whether it's completely correct — or completely fabricated.

This isn't a bug. It's how the technology works.

Generative AI predicts the most plausible next word. It is not designed to verify truth.

AI ASSISTANT — RESPONSE

*"Based on established Illinois statute 720 ILCS 5/11-204.1, the elements of aggravated fleeing and eluding are: (1) the officer was in uniform, (2) the officer activated lights, (3) the defendant increased speed, and (4) property damage or injury resulted. This is well-settled law."*

**UNVERIFIED**

### Probability

AI outputs are based on probability — not fact.

### No Warning Signal

There's no flag that tells you when it's wrong.

The risk isn't that AI lies. The risk is that it sounds like it's telling the truth — every single time.

# This Happens in Court

## CASE STUDY — HALLUCINATIONS IN COURT FILINGS

### Alabama paid a law firm millions to defend its prisons. It used AI and turned in fake citations

Butler Snow faces sanctions after lawyer cites false case law defending against inmate who says he was stabbed 20 times

#### ~1,000 documented cases

*of AI hallucinations submitted in actual court filings*

AI systems agree with you even when you're wrong. The "Confidence Paradox": every response sounds authoritative — whether it's correct or completely fabricated.

*Source: AI Law Librarians / Legal Research Review*

## SANCTIONS & FINES — FEBRUARY 2026

### US appeals court orders lawyer to pay \$2,500 over AI hallucinations in brief

By Nate Raymond

#### US Appeals Court orders lawyer to pay \$2,500

*over AI hallucinations in brief — Reuters, Feb. 18, 2026*

An attorney submitted AI-generated case citations that did not exist. The court sanctioned the attorney personally. Defense attorneys in your jurisdiction are watching for exactly this.

*Source: Reuters / US Court of Appeals*

These aren't edge cases. They're happening now — in courtrooms that handle your cases.

# AI Is Not Inherently Reliable



AI OUTPUT

**Plausible**  
**Confident**  
**Sometimes Wrong**

Outputs are based on probability,  
not absolute truth.

AI can be confident and wrong simultaneously.

TRUST  
BUT  
VERIFY

YOUR RESPONSIBILITY

**Verify.**  
**Every time.**  
**No exceptions.**

The risk is not hallucination.

The risk is **unverified AI output driving a law enforcement action.**

Trust but Verify is a professional obligation — not a suggestion. Document your verification process every time.

# When Verification Fails

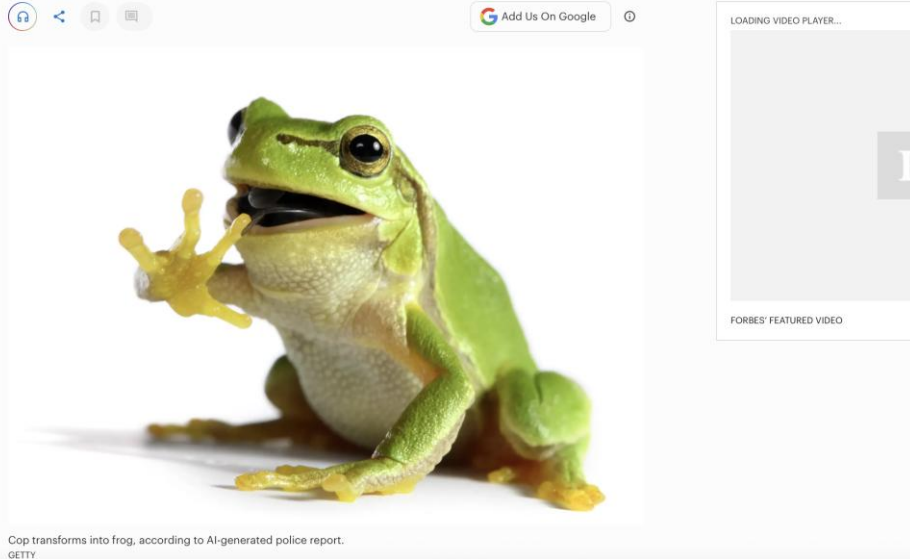
Forbes

## Cop Transforms Into Frog, According To AI-Generated Police Report

By [Lars Daniel](#), Contributor. © Lars Daniel covers digital evidence and forensics in ...

[Follow Author](#)

Published Jan 04, 2026, 01:18pm EST, Updated Jan 05, 2026, 12:52pm EST



Cop transforms into frog, according to AI-generated police report.  
GETTY

## US student handcuffed after AI system apparently mistook bag of chips for gun

Baltimore county high schools have gun detection system that alerts police if it sees what it deems suspicious



Kenwood High School in Essex, Maryland. Photograph: Google Maps

An **artificial intelligence system** (AI) apparently mistook a high school student's bag of Doritos for a firearm and called local police to tell them the pupil was armed.

Taki Allen was sitting with friends on Monday night outside Kenwood high school in **Baltimore** and eating a snack when police officers with guns approached him.

# COURTOOM EXAMPLE



U.S. ▾

Politics ▾

World ▾

Opinion

Media ▾

Entertainment ▾

Sports ▾

Lifestyle ▾

ARTIFICIAL INTELLIGENCE

## AI-generated attorney outrages judge who scolds man over courtroom fake: 'not a real person'

A New York man found himself in hot water after he used an AI-avatar to argue his case in front of a panel of judges



By Julia Bonavita · Fox News

Published April 9, 2025 10:57am EDT

<https://www.foxnews.com/us/ai-generated-attorney-outrages-judge-who-scolds-man-over-courtroom-fake-not-real-person>



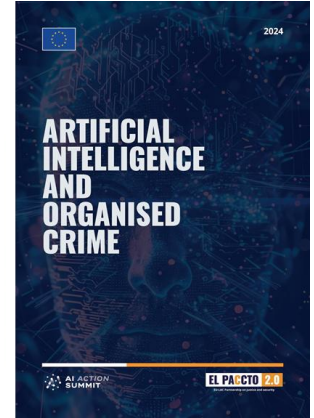
#IACP2026

# CRIMINAL USE OF AI



# Criminal use of AI

- Online financial fraud
- Online sexual exploitation (CSAM, children)
- Extortion / sextortion / sexting
- Virtual kidnapping
- Cyberattacks on infrastructure
- Disinformation campaigns
- Criminal use of analytics
- Full “kill chain” with AI agents



# Criminal use of AI

Category	What it does	Examples
<b>AI as a weapon</b>	Direct execution of the offence	Deepfakes, phishing-texts, voice clones, malware generation
<b>AI as a scout</b>	Identifying and compromising targets	OSINT-automating, vulnerability scanning, building profiles
<b>AI as a facilitator</b>	Supports the criminal process	Translate scam messages, code malware, optimize laundering
<b>AI as a shield</b>	Avoid detection	Polymorph malware, deepfake for KYC-bypass, anti-forensics

# Bank fraud with fake id's



## Dutch Police Arrest 8 in Fake ID Platform Probe

NEWS

Using server data seized in a raid last year, Dutch authorities arrested eight people this week for their roles in a massive international fake ID ring.



Banner: Annette Riedl/DPA/dpa Picture-Alliance via AFP

Reported by  
**James Dowsett**  
OCCRP

April 10, 2026



Dutch police arrested eight men on suspicion of identity fraud, forgery and cybercrime this week in connection with a multi-million-dollar fake ID platform that generated nearly a million forged documents for scammers worldwide.

The nationwide operation, carried out on April 7 and 8, targeted users of VerifTools, a now-shuttered website that allowed users to enter false

## Man opened 46 bank accounts using deepfakes and stolen IDs

March 18, 2026



ABN Amro offices in Rotterdam. Photo: Depositphotos.com

A man created 46 bank accounts in other people's names using deepfake technology to bypass face recognition software, a court has been told.

The Dutch man used doctored images of his own face to deceive ABN AMRO's identity check mechanism, which asks applicants to submit photo ID such as a passport or identity card and verify it by taking a selfie.



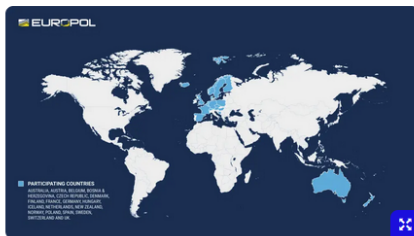


NEWS

# 25 arrested in global hit against AI-generated child sexual abuse material

28 FEB  
2025

Europol has supported authorities from 19 countries in a large-scale hit against child sexual exploitation that has led to 25 arrests worldwide. The suspects were part of a criminal group whose members were engaged in the distribution of images of minors fully generated by artificial intelligence (AI).



Most of the arrests were carried out simultaneously on 26 February 2025 during a global operation (Operation Cumberland) led by Danish law enforcement. More arrests are expected in the coming weeks, as the operation is still ongoing.

## Results of the operation, so far:

- 273 suspects identified
- 25 suspects arrested



NOS Nieuws • Woensdag 13 augustus, 08:47



## Politie heeft maker en opdrachtgever van deepfake video van BN'ers in beeld

De politie heeft een 73-jarige man uit Noord-Holland in beeld die een deepfake pornovideo van een bekende Nederlander zou hebben gemaakt. Dat bevestigt het OM na berichtgeving in het AD.

Het OM is nog in afwachting van het onderzoeksdossier. Als dat binnen is, neemt het een beslissing over vervolging van de man.

Volgens de krant werkte de man in opdracht van een Canadees uit Toronto die een internationale website runde waarop dit soort video's waren te zien.

### MrDeepFakes

Het OM begon vorig jaar een onderzoek naar de website die de deepfake video's maakte. Het bericht in dezelfde krant. Daarin stond dat op de site namen van tientallen bekende Nederlanders uit de showbizz, tv-wereld en de politiek waren te zien.



# INTERPOL report warns of increasingly sophisticated global financial fraud threat

16 March 2026

[Home](#) > [News and Events](#) > [News](#) > [2026](#) > [INTERPOL report warns of increasingly sophisticated global financial fraud threat](#)

## Threat assessment highlights hybrid tactics, global growth in scam centres and rise in sextortion

Financial fraud is now one of the world's most severe and rapidly evolving transnational crimes, with significant economic and human consequences.

The 2026 INTERPOL Global Financial Fraud Threat Assessment warns that with increased global criminal collaboration, fraud is no longer a peripheral threat, it is at the centre of polycriminality, intersecting with organized crime, human trafficking and cybercrime.

Key findings include:

- **AI-enhanced fraud** is 4.5 times more profitable than traditional methods. "Agentic AI" systems can autonomously plan and execute complete fraud campaigns - from reconnaissance to ransom demands.
- **Sextortion** is now being systematically integrated into scams such as romance and investment fraud often using scripts and AI-generated content.
- **Criminal networks are increasingly collaborating** with specialized money laundering groups and sharing expertise and technology to scale up their operations globally.
- In parts of Africa, **terrorist groups** have been found to use fraud schemes, especially crypto-based scams, as a source of funding.
- Once a regional phenomenon, **scam centres** have now been identified worldwide, involving hundreds of thousands of individuals, many of whom are trafficked and forced to carry out online fraud.



# INTERPOL report warns of increasingly sophisticated global financial fraud threat

16 March 2026

[Home](#) > [News and Events](#) > [News](#) > [2026](#) > [INTERPOL report warns of increasingly sophisticated global financial fraud threat](#)

## Threat assessment highlights hybrid tactics, global growth in scam centres and rise in sextortion

Financial fraud is now one of the world's most severe and rapidly evolving transnational crimes, with significant economic and human consequences.

The 2026 INTERPOL Global Financial Fraud Threat Assessment warns that with increased global criminal collaboration, fraud is no longer a peripheral threat, it is at the centre of polycriminality, intersecting with organized crime, human trafficking and cybercrime.

• **AI-enhanced fraud** is 4.5 times more profitable than traditional methods. “Agentic AI” systems can autonomously plan and execute complete fraud campaigns - from reconnaissance to ransom demands.

fraud campaigns - from reconnaissance to ransom demands.

- **Sextortion** is now being systematically integrated into scams such as romance and investment fraud often using scripts and AI-generated content.
- **Criminal networks are increasingly collaborating** with specialized money laundering groups and sharing expertise and technology to scale up their operations globally.
- In parts of Africa, **terrorist groups** have been found to use fraud schemes, especially crypto-based scams, as a source of funding.
- Once a regional phenomenon, **scam centres** have now been identified worldwide, involving hundreds of thousands of individuals, many of whom are trafficked and forced to carry out online fraud.



# EVOLUTION OF AI MODELS IN CYBERCRIME



Maligned Models

- WormGPT
- FraudGPT
- DarkBERT

Jailbreaking Frontier Models

- EscapeGPT
- LoopGPT
- BlackhatGPT

Compromising Agents

- Clawhavoc
- Atomic Stealer
- GhostSocks

# AI: criminal catalyst, not just a tool

AI is a criminal catalyst, not just a tool.  
Hierarchies are becoming digital architectures.  
Crime is becoming "faceless."

## Sinaloa Cartel and CJNG

- AI to optimize drug and human trafficking routes
- conduct financial fraud
- and automate emotional extortion

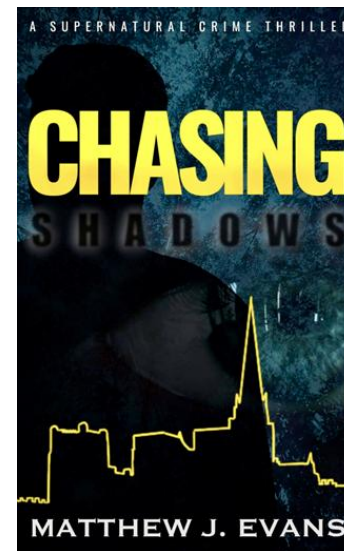
## KK Park scam-factories

- hybrid models of algorithmic criminal governance
- militias, criminal capital, and AI converge

Autonomous platforms, such as **FunkSec** and **Xanthorox AI**, are blurring the lines between perpetrator and system.

<https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/>

<https://www.varonis.com/blog/xanthorox-ai>



# CSAM CREATION

## AI ALLOWS FOR THE CREATION OF CSAM IN SEVERAL WAYS



know2  
protect®



Homeland  
Security  
Investigations

- \* Take an image of a child and make it appear as though the child is nude or engaged in sexual acts
- \* Create an image of a child being sexually abused via text prompts
- \* Manufacture images of children being abused who look like real people but are fabricated
- \* Teach other offenders how to engage with children online (i.e., grooming)
- \* Revictimize CSAM victims: using AI to edit previously created and shared content to create new CSAM



THE RISE OF  
cybercrime-as-a-service



# CHANGLIN SLIDES + DEMO

#IACP2026

# AI Safety Awareness Project



- Nonprofit doing pro bono workshops for the general public and various other institution
  - Law enforcement agencies
  - Other municipal and state government departments
- Universities, schools, churches, technology companies
- Both technical and non-technical workshops
- Network of volunteers around the U.S.

# Setting the Stage



Who here has thought about deepfakes?

# Setting the Stage



Who here has thought about AI misinformation campaigns? Fake videos or fake-news of a law enforcement/civilian interaction?

# Setting the Stage



Who here has thought about the first time a trail of evidence leads you not to a human suspect, but to an autonomous AI system?

# AI Moves Quickly!

AI Video in 2023:



#IACP2025

# AI Moves Quickly!

AI Video in 2025:



#IACP2025

# Cybersecurity Demo

<https://research.civai.org/>



#IACP2025

# What is “AI Safety”



## Proactively Addressing Risk

- Exacerbating pre-existing societal problems
- Unprecedented social/economic impacts
- How to make sure AI doesn't endanger humanity

# What is AGI: Artificial General Intelligence



- Ill-defined, but some overlap
- OpenAI: “autonomous system that **outperforms humans at most economically valuable work**” [OpenAI](#)
- Demis Hassabis, CEO of DeepMind: “should be able to do pretty much **any cognitive task that humans can do.**” From [Science Friday](#)
- **A lot of uncertainty remains!**
  - But this is what AI companies are explicitly trying to make

# AI Companies believe they will create AGI very soon

These next three years might be the last few years that I work. I am not ill, nor am I becoming a stay-at-home mom, nor have I been so financially fortunate to be on the brink of voluntary retirement. I stand at the edge of a technological development that seems likely, should it arrive, to end employment as I know it. - **Avital Balwit**, Chief of Staff to the CEO, Anthropic, May 2024

We have set internal goals of having an automated AI research intern by September of 2026 running on hundreds of thousands of GPUs, and a true automated AI researcher by March of 2028. - **Sam Altman**, CEO of OpenAI, Jan 2025

# AI Companies believe they will create AGI very soon



#IACP2025

# Capabilities Trend



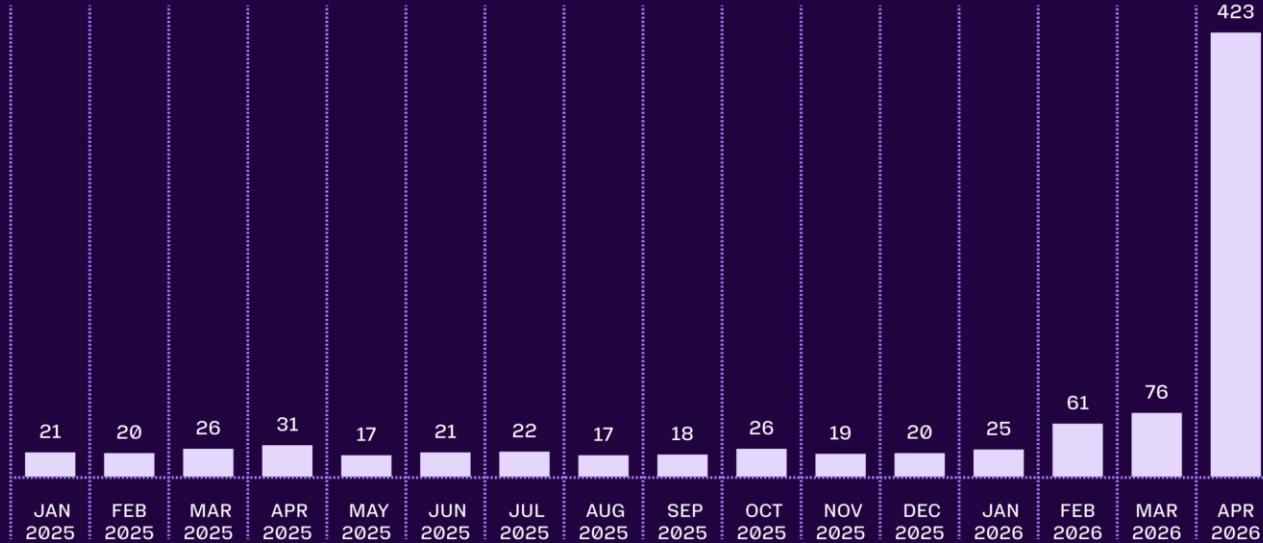
- Last 40 days have seen large progress
  - Claude Mythos
  - GPT 5.5
  - (Not yet released at time of edit, but will likely be released on day of presentation) Next generation of Google Gemini + Google Spark
  - Models that are able to upend usual cybersecurity assumptions
- Difficult to evaluate because models have not been made publicly available
  - But signs indicate continuing exponential progress

# Capabilities Trend



## Firefox Security Bug Fixes by Month

All Sources • All Severities



#IACP2025

# Capabilities Trend



National Cyber  
Security Centre

[About NCSC](#)

[Report an incident](#)

[Contact us](#)



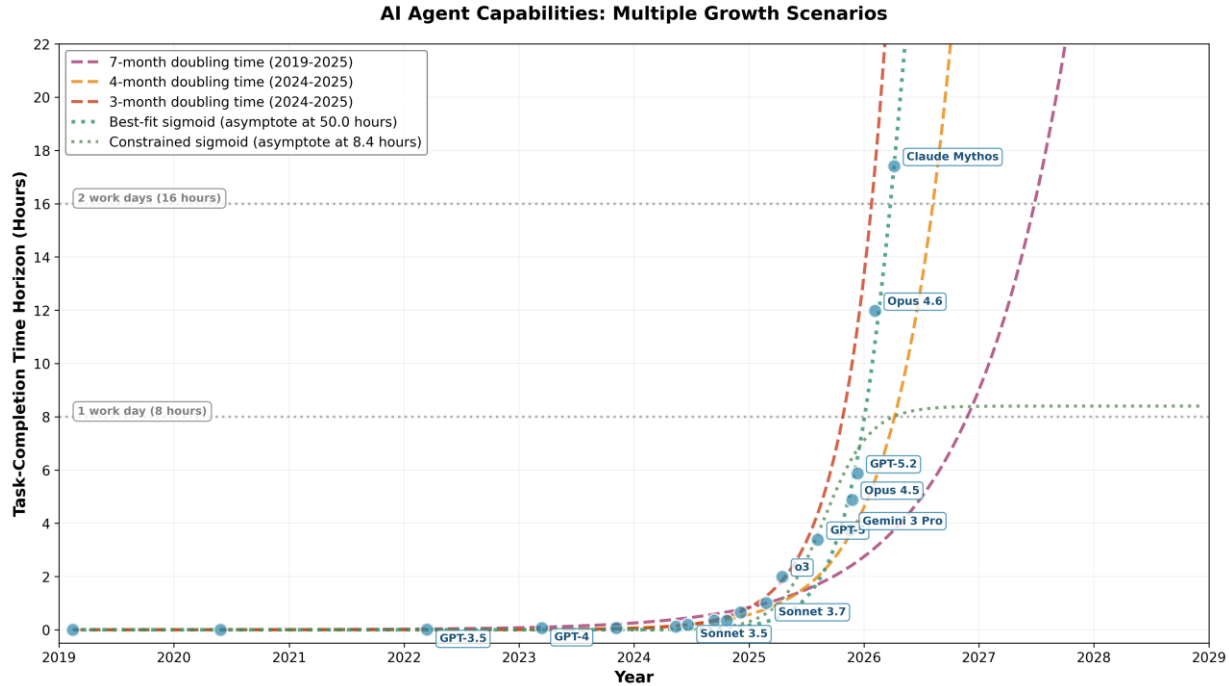
## Preparing for a 'vulnerability patch wave'

Organisations must act now to prepare for a wave of patches that will address decades of technical debt.

May 1, 2026

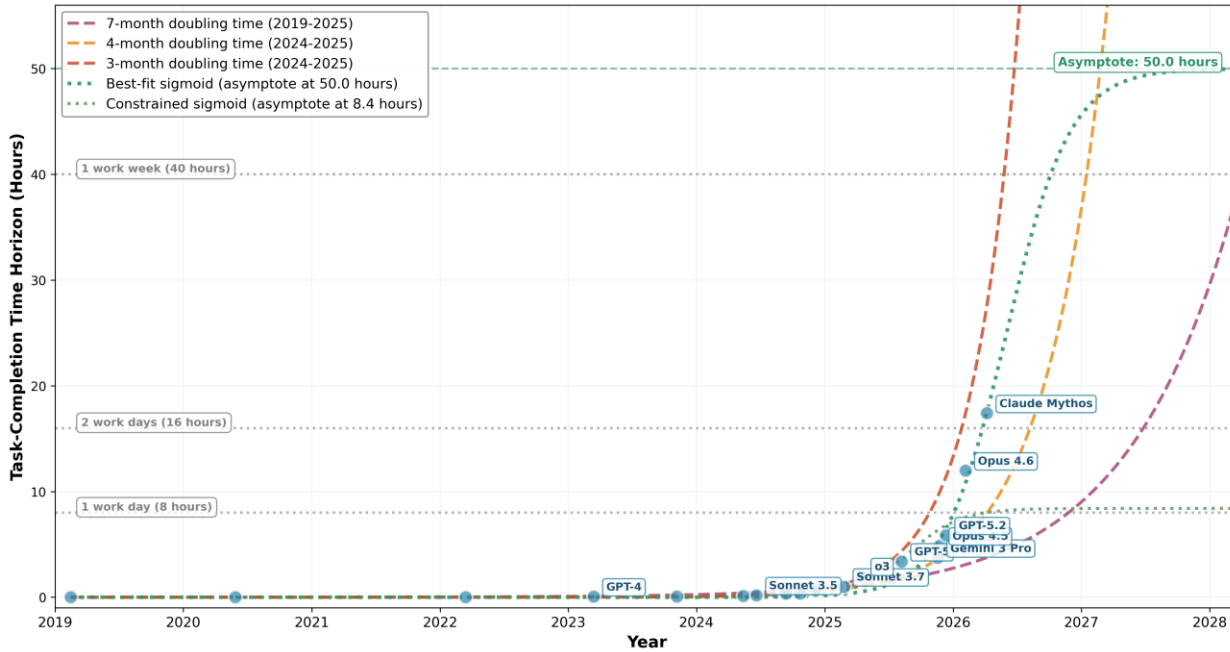
#IACP2025

# Capabilities Trend

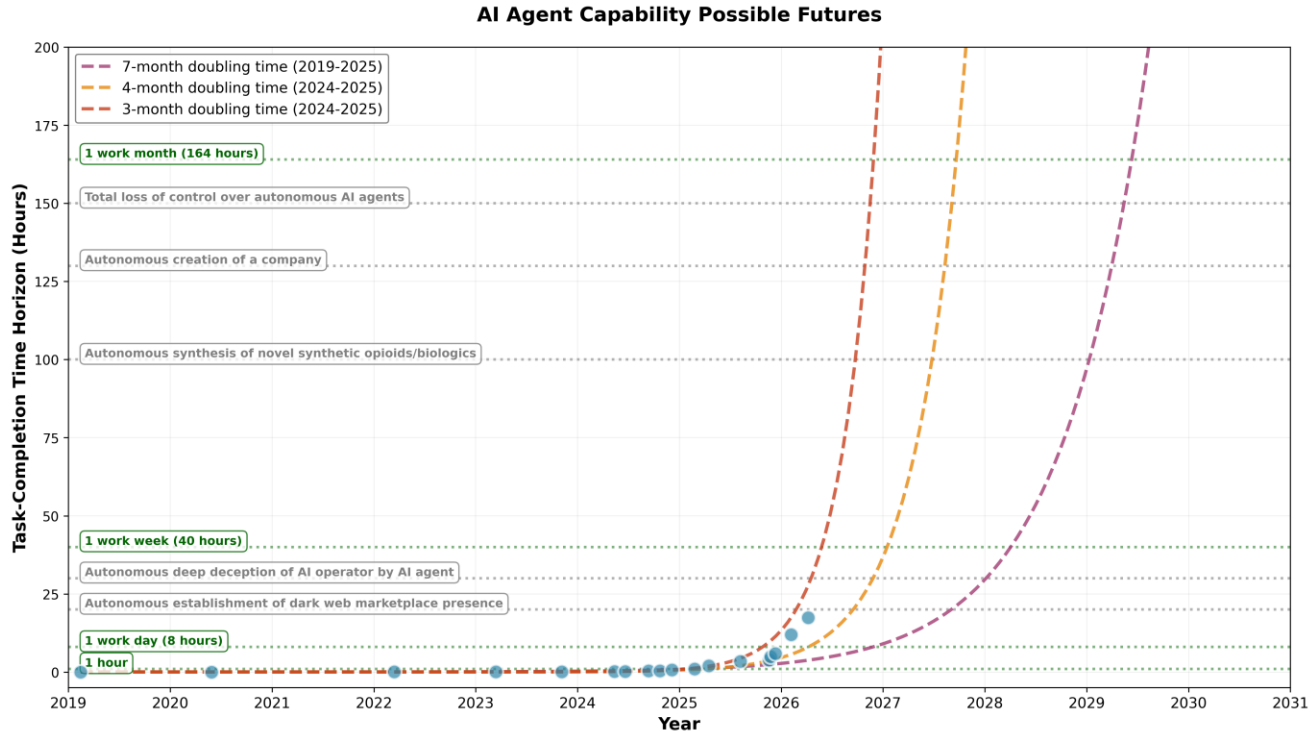


# Capabilities Trend

AI Agent Capabilities: Best-Fit Sigmoid Full Trajectory



# Capabilities Trend



# Potential Danger Ahead



**No one knows how modern AIs actually work:** Grown not built

**Yoshua Bengio**, Turing Award winner

"...nobody currently knows how such an AGI could be made to behave morally, or at least **behave as intended by its developers and not turn against humans**... As of now, however, we are racing towards a world with entities that are smarter than humans and pursue their own goals – without a reliable method for humans to ensure those goals are compatible with human goals."

Median AI expert believes **10% chance that AI will cause human extinction** (2023)

[Alimpacts](#)

# Almost Everyone is Behind the Curve

- AI is moving extremely quickly
- Bad actors are behind
  - Only sophisticated actors are keeping up
  - But they're catching up!
- You have a chance to get ahead of the curve

# What can you do as an org?



- Building situational awareness of where AI is and where it's going
- Positioning your organization as a trusted source of expertise for your community
- Making your voice heard on the larger national stage
- But there's a closing window of opportunity

# More Info



#IACP2025

# Presenters

---

## Jonathan Lewin



### Contact:

[jonathan.lewin@outlook.com](mailto:jonathan.lewin@outlook.com)

**+1 773-220-9999**

Jonathan Lewin is an Associate Consultant at 21CP Solutions (21st Century Policing LLC). Prior to this role, he was a Domain Lead with a focus on artificial intelligence, situational awareness, and CJIS integration at the First Responder Network Authority. He was Executive Officer for Operations and Acting Deputy Director at INTERPOL Washington, an agency of the U.S. Department of Justice. Lewin retired from the Chicago Police Department as Chief of the Bureau of Technical Services following a 28-year career as a sworn member. He represented the Major Cities Chiefs Association on FirstNet's Public Safety Advisory Committee and served on the International Association of Chiefs of Police (IACP) CJIS Committee. Lewin was named Technology Champion of the Year by the National Organization of Black Law Enforcement Executives (NOBLE) and recognized as one of Government Technology's Top 25 Doers, Dreamers & Drivers. He has presented nationally on emerging public safety technology topics and holds an M.A. in Security Studies from the Naval Postgraduate School, an M.A. in Public Policy from Northwestern University, and a B.S. in Administration of Justice from Southern Illinois University.

# Presenters

---

## Oscar Wijsman



**Contact:**

[oscar.wijsman@politie.nl](mailto:oscar.wijsman@politie.nl)

**+31 6 2876 3252**

Oscar Wijsman is the international AI & Data Science Lead of the Netherlands Police. Within the police and for other law enforcement agencies and partners, he is a central point of contact for data science, artificial intelligence & advanced analytics-related topics. His areas of focus are organisational development, technical infrastructure, legislation, governance, general coordination, policy making and analytics developments.

Oscar is chair of the Europol EuCB Strategic Group on AI and a member of the IACP Communication & Technology Committee and chair of its AI Subcommittee. He holds a BSc in Automotive Technology and Computer Science and a postgraduate degree in Accounting Information Systems.

# Presenters

---

## Changlin Li



Changlin is the Executive Director of the AI Safety Awareness Project. He began his career at the Systemized Intelligence Lab at Bridgewater Associates for 5 years before joining Vowel.com (now acquired by Zapier) as a founding engineer for 4 years. Along the way he did a stint at the Recurse Center in New York City studying formal verification of software and then another stint at the Recurse Center with a focus on modern AI and AI safety. He holds an A.B. in Mathematics with a Secondary Concentration in Comparative Religion from Harvard University.

### Contact:

[changlin@aisafetyawarenessproject.org](mailto:changlin@aisafetyawarenessproject.org)

+1 425 591 4476

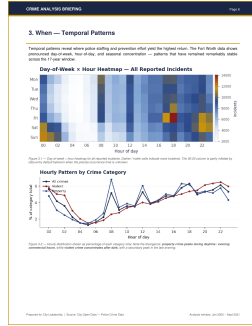
SAMPLE OUTPUT Below: actual pages from a 15-page briefing produced from a 1.16M-record municipal crime dataset



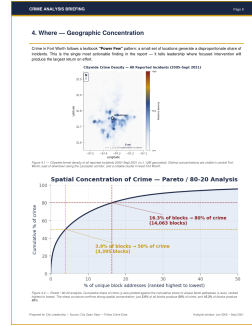
Cover Key Findings at a Glance



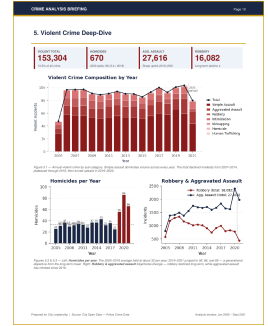
Executive Summary KPI cards + caveats



Temporal Patterns DOWxHour heatmap



Geographic KDE hotspot + Pareto



Violent Deep-Dive Composition + homicide

What's inside → Cover with at-a-glance bullets (Major Findings / Trends / Correlations / Projections) • Executive summary with KPI cards • Annual & monthly trends + 12-month moving average • Top crime types color-coded by category • DOWxHour heatmaps • Geographic concentration (KDE hotspot maps, Pareto 80/20 curve, top blocks) • Violent & property deep-dives • Linear projection with caveat • Findings, methodology, & stated limitations

THE PROMPT Paste into a new Claude chat with your dataset attached. Claude inspects the data, adapts the analysis to what's available, and produces the PDF.

```
You are a senior crime analyst. I'll attach a crime/incident dataset (CSV, Excel, or similar). Produce a polished PDF briefing ('Crime_Analysis_Briefing.pdf') suitable for command staff, elected officials, or community stakeholders - 12-16 pages, plain language, strong visuals, defensible numbers.

# CORE PRINCIPLE
Don't assume the schema. Inspect the data first, figure out what's actually there, and shape the analysis around what the data supports. Don't ask clarifying questions unless the file is unreadable - proceed, make reasonable choices, document them in the report.

# STEP 1 - DATA DISCOVERY (before any chart code)
Load a sample and report briefly:
- File shape, rows, column names, dtypes
- For each column: % populated, sample values, apparent meaning
- Identify the analytical fields: date/time, offense/crime-type, location, premise type, anything else useful
- Effective date range; flag if recent months are partial/stale
- Obvious gaps or suppression (e.g., sex offenses missing)
Continue even if some fields are missing. Surface caveats in the report.

# STEP 2 - CRIME CLASSIFICATION (adapt to data)
Group offenses into three FBI/NIBRS-aligned buckets:
- VIOLENT: homicide, assault, robbery, intimidation, kidnapping, human trafficking, sex offenses if present
- PROPERTY: burglary, larceny/theft, MVT, theft from MV, vandalism, arson, fraud, forgery, embezzlement, stolen property
- SOCIETY/ORDER: drug & narcotic, DUI/DWI, weapons, prostitution, disorderly conduct, trespass, liquor, gambling, warrants
If NIBRS/UCR codes → use the official taxonomy. If only free-text → keyword classifier covering ≥95% of records. If only call-types → group by best judgment and disclose mapping. Show logic in methodology.

# STEP 3 - LOCATION HANDLING (whatever data supports)
Geographic analysis tier - use the highest the data supports:
TIER 1: lat/lon → KDE hotspot maps + scatter density
TIER 2: addresses → geocode sample via Nominatim/OSM
TIER 3: addresses only, no geocoding → block-level concentration, Pareto curve, beat/district aggregation, top-20 block bar chart
TIER 4: no location → drop geo section; expand temporal/offense
Always do block-level Pareto if any location string exists.

# STEP 4 - REQUIRED ANALYSES (skip cleanly if unsupported)
1. Annual trend stacked by category + monthly 12-mo moving average; band any obvious era (COVID, policy change)
2. Top 15 offense types color-coded by category
3. Category composition donut + plain-English bucket explanation
4. Temporal (if time-of-day exists): DOWxHour heatmap, hour-curve comparing violent vs property, DOW bars, monthly seasonality

5. Geographic concentration - scale to tier from Step 3
6. Top blocks + premise/location-type breakdown (if present)
7. Violent deep-dive: KPI cards, stacked yearly composition, homicide per year, robbery vs agg-assault, violent timing & geography
8. Property deep-dive: KPIs, yearly composition, burglary/MVT/theft trend lines, property timing
9. Projection: linear fit full-year + recent-5yr slope, directional indicator only - call out aggregate vs category-level divergence
If a section's data is unavailable, note what would be needed.

# STEP 5 - VISUAL STYLE
Command-briefing palette: Navy #1a2744, Gold #c9960c, Red #8b1a1a (violent), Blue #2c4a8c (property). Clean sans-serif, minimal spines, no chart junk. Legends OUTSIDE plot area on stacked charts. Donut # labels OUTSIDE wedges. Annotations in clean whitespace, never on top of dashed reference lines. KDE colormap: white→blue→gold→red. Letter size, ~0.6" side margins, ~0.85" top margin.

# STEP 6 - PDF STRUCTURE
1. COVER - navy header, title, KEY FINDINGS AT A GLANCE with gold underline; bullets grouped MAJOR FINDINGS / TRENDS / CORRELATIONS / PROJECTIONS
2. Executive Summary - 4 KPI cards, narrative, What's up / What's down / Where it concentrates columns, data caveats callout
3. Overall Trend & Category Mix
4. Primary Crime Types
5. Temporal Patterns (omit if no time-of-day)
6. Geographic Concentration (scale to Tier from Step 3)
7. Top Blocks + Location Types
8. Violent Crime Deep-Dive
9. Violent Timing & Geography
10. Property Crime Deep-Dive
11. Trend Lines & Forward Look
12. Findings + Methodology + Stated Limitations
Use ReportLab 'KeepTogether' to bind charts with captions and headers with content. Consolidate aggressively - no orphan captions.

# STEP 7 - QUALITY BAR (before delivery)
- Render every page to PNG and visually verify
- Check: legend-overlapping-bars, axis-tick collisions, orphaned captions, donut labels obscuring center text, off-page elements
- If a page is mostly whitespace, shrink prior chart or consolidate - Aim for ≤16 pages total

# OUTPUT
Save: `mnt/user-data/outputs/Crime_Analysis_Briefing.pdf`. Then give a one-paragraph summary of what you produced, what choices you made (e.g., "no coordinates → Tier 3 block-level concentration"), and what's NOT included due to data limitations.
Begin by inspecting the file.
```

MODIFICATIONS Append any of these to the prompt above to customize for your situation

- Small dataset (<10k records). "Don't attempt KDE smoothing or projections — sample size insufficient. Show raw counts and percentages only."
Different output format. "Output as an interactive HTML dashboard" OR "Output as a PowerPoint deck with one chart per slide."
Campus / single-precinct data. "Frame as operational rather than citywide — reference deployment, patrol, prevention rather than 'city leadership'."
Custom branding. "Use [agency name] on the cover; replace navy/gold palette with [your colors]."
Specific audience. "Target audience is [city council / sheriff / community advisory board]" — adjusts tone and what counts as actionable.
Add comparison context. "Where possible, contextualize trends against state / FBI national rates for the same offense categories."

# PUBLIC SAFETY AI PROMPT LIBRARY

## Law Enforcement Edition

**Jonathan Lewin**

Powered by Claude • April 2026

11 ready-to-use AI prompts for law enforcement professionals. Each prompt works in a fresh Claude or ChatGPT conversation — paste it in, answer a few intake questions, and the AI tells you exactly what data to upload and produces a complete, usable output.

- ① Open a fresh Claude (claude.ai) or ChatGPT (chat.openai.com) conversation
- ② Copy the prompt box from any page and paste it into the chat
- ③ The AI asks structured intake questions about your agency and data
- ④ Follow the AI's instructions — it tells you exactly what to upload
- ⑤ The AI produces a complete, usable output — report, tool, draft, or analysis
- ⑥ Review all outputs carefully before any operational, legal, or administrative use

■■ EDUCATIONAL USE ONLY. These prompts and outputs are provided for training and professional development purposes. They do not constitute legal, operational, or policy advice.

■■ REVIEW ALL OUTPUTS. AI systems make errors. Always verify AI-generated content for accuracy, policy compliance, and legal sufficiency before any operational or administrative use.

■■ CJIS COMPLIANCE. Do not submit raw CJIS-protected data, PII, biometric records, or NCIC returns to any external AI service. Sanitize and anonymize all data before uploading.

■■ AGENCY POLICY. Verify AI tool use complies with your agency's AI use policy, collective bargaining agreement, procurement requirements, and applicable law.

■■ NO ENDORSEMENT. Mention of Claude or ChatGPT is not a product endorsement. Evaluate all platforms against your agency's data security and procurement requirements.

PROMPTS 1-7		PROMPTS 8-11 ★ = multi-page	
1	Command Crime Briefing Generator	8	Use of Force Summary Generator
2	Crime Hotspot & Patrol Deployment	9	Training Scenario Generator
3	Patrol Shift Schedule Optimizer	10	Staffing & Coverage Gap Analysis
4	Officer & Squad Productivity	11	Crime Mapping Dashboard Builder ★
5	Grant Writing Assistant		
6	AI Policy Draft Generator		
7	AI Policy Gap Analyzer		

## 1 Command-Level Crime Briefing Generator

Analyzes your agency's crime data and produces a publication-quality executive briefing with KPI summary, ranked hotspot analysis, temporal patterns, trend comparison, and evidence-based deployment recommendations. Suitable for CompStat, city leadership, or board presentations.

**What this produces:** A structured PDF-ready briefing with executive summary, hotspot table, day-of-week and hour-of-day charts, offense breakdown, trend comparison, and deployment recommendations citing peer-reviewed research.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are a professional crime analyst and law enforcement intelligence specialist.  
I want to generate a command-level crime analysis briefing from my agency's incident data.

**STEP 1 – ASK ME THESE QUESTIONS BEFORE I UPLOAD ANYTHING:**

1. What is your agency name and jurisdiction? (for the report header)
2. What time period does the data cover? (e.g., Q1 2026, or Jan-Mar 2026)
3. Do you have a prior-period comparison dataset? (for trend analysis)
4. What crime types are included? (all crimes, violent only, property only, etc.)
5. Who is the audience? (chief/sheriff, city manager, council, community board)
6. Are there specific questions leadership is asking you to answer?
7. Does your data include beat/district assignments?

**STEP 2 – TELL ME WHAT FILE TO UPLOAD:**  
Based on my answers, tell me exactly what format and columns my file needs.  
Remind me to: remove all PII (names, DOB, SSN, case numbers), remove victim/witness addresses, use block-level locations only, and aggregate sensitive categories.

**STEP 3 – ONCE I UPLOAD THE DATA, PRODUCE A COMPLETE BRIEFING INCLUDING:**

- EXECUTIVE SUMMARY: 3-4 bullet key findings a chief can read in 60 seconds
- KPI DASHBOARD: Total incidents, % change vs. prior period, clearance rate (if available)
- TOP HOTSPOT TABLE: Top 10 locations ranked by count, with % of total and trend arrow
- RISING THREATS: Locations with >20% increase vs. prior period flagged in red
- TEMPORAL ANALYSIS: Peak day of week, peak 4-hour window, shift-by-shift breakdown
- OFFENSE BREAKDOWN: Count and % by crime type, sorted by volume
- BEAT/DISTRICT SUMMARY: Incident distribution across patrol zones (if data available)
- TREND COMPARISON: Current vs. prior period by crime type with % change
- DEPLOYMENT RECOMMENDATION: 3-5 specific, evidence-based recommendations citing established research (hot spots policing, focused deterrence, etc.)
- DATA NOTES: Acknowledge any data limitations or caveats

**FORMAT REQUIREMENTS:**

- Use professional law enforcement report language – clear, active voice, no jargon
- Bold all key numbers and findings
- Use only real, verifiable research citations (Braga et al., Weisburd et al., etc.)
- Flag any figures that seem anomalous and ask me to verify before finalizing
- End with a section the chief can read aloud as talking points

**OUTPUT FORMAT:** Build as an interactive HTML artifact (renders live in Claude chat).  
Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.

It opens in your web browser (Chrome or Edge) – looks exactly like this.

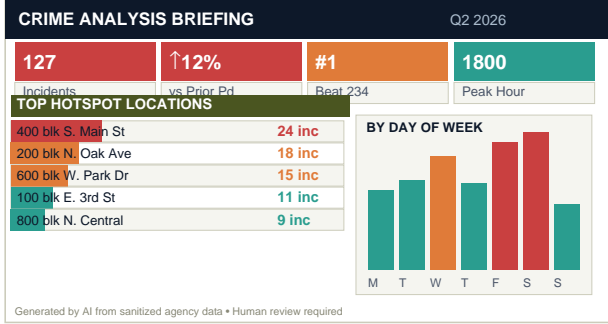
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac). Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- Crime incident CSV or Excel: incident date/time, offense type, block-level address or beat/zone
- Optional: prior period comparison file (same format) for trend analysis
- Optional: clearance/disposition codes if available
- REMOVE before uploading: victim names, witness info, officer names, case/DR numbers, exact addresses
- Use block-level addresses only (e.g., '400 blk N. Main St') — never exact street numbers

**SAMPLE OUTPUT**



■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 2 Crime Hotspot & Patrol Deployment Analysis

Identifies your agency's highest-risk locations using spatial concentration analysis, maps crime to time windows and patrol beats, and produces evidence-based deployment recommendations grounded in hot spots policing research. Outputs a ranked hotspot file, beat-level summary, and ready-to-use supervisor briefing.

**What this produces:** Ranked top-10 hotspot table, rising vs. declining hotspot trend analysis, peak day/hour heat map data, beat-level distribution, patrol allocation recommendations with supporting research citations.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are an expert crime analyst specializing in spatial crime analysis, hotspot identification, and evidence-based patrol deployment strategy.

**STEP 1 – ASK ME THESE QUESTIONS BEFORE I UPLOAD ANYTHING:**

1. What geographic area does my patrol zone cover? (city, precinct, campus, district)
2. What time period should the analysis cover? (90 days, 6 months, 1 year)
3. Should I focus on all crimes, or specific offense types? (violent crime, robbery, auto theft, commercial burglary, etc.)
4. Do I want a focus on a specific time window? (e.g., evening hours 1800-0200)
5. Do I have year-over-year or prior-period comparison data?
6. Does my data include beat or district codes?
7. What problem am I trying to solve with this analysis? (coverage gaps, surge planning, CompStat prep, resource justification)

**STEP 2 – TELL ME WHAT TO UPLOAD:**  
Based on my answers, specify the exact file format and required columns. Remind me to use block-level addresses only and remove all PII.

**STEP 3 – ONCE I UPLOAD THE DATA, PRODUCE:**

- **TOP 10 HOTSPOT LOCATIONS:** Ranked by incident count with % of total crime, exact block address, primary offense types at each location
- **SPATIAL CONCENTRATION:** What % of crimes occur in the top 5% of locations? (Benchmark: research shows ~50% of crime in ~5% of addresses)
- **RISING vs. DECLINING HOTSPOTS:** Compare current to prior period, flag locations with >25% increase as Priority 1 targets
- **TEMPORAL HEAT MAP DATA:** For top 5 hotspots, show their specific peak hours and days – not just agency-wide peaks
- **BEAT/DISTRICT BREAKDOWN:** Incidents per beat, % of total, top offense per beat
- **PATROL RECOMMENDATIONS:** For each Priority 1 hotspot, recommend:
  - Optimal patrol windows (based on actual peak hours at that location)
  - Suggested patrol tactic (presence patrol, directed patrol, problem-solving)
  - Relevant evidence-based intervention (cite Braga, Weisburd, Sherman, etc.)
- **SUPERVISOR BRIEFING BULLET POINTS:** 5 bullets a sergeant can use at roll call

**CITE ONLY** verified research from: Campbell Systematic Reviews, Journal of Experimental Criminology, Criminology & Public Policy, or equivalent.

**OUTPUT FORMAT:** Build as an interactive HTML artifact (renders live in Claude chat). Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

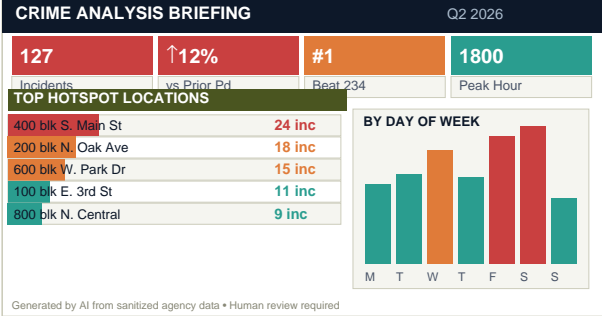
1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it. It opens in your web browser (Chrome or Edge) – looks exactly like this.
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac). Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- Incident CSV/Excel: date, time, offense type, block-level address or lat/lon
- Optional: beat/district code per incident; prior period comparison file
- Block-level addresses only — no exact house numbers, no victim/witness addresses
- REMOVE: all names, case numbers, DOB, SSN, phone numbers, license plate numbers

**SAMPLE OUTPUT**



**■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.**

### 3 Patrol Shift Schedule Optimizer

Designs an optimized patrol shift schedule aligned to your agency's actual calls-for-service demand, CBA constraints, and staffing levels. Analyzes your CAD data to identify peak coverage needs, then produces a mathematically sound rotation that satisfies labor agreement requirements while maximizing officer presence during high-demand periods.

**What this produces:** Optimized 28-day shift calendar, coverage analysis vs. CFS demand, peak-hour alignment report, CBA constraint verification, and a plain-language summary for command staff or union presentation.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

#### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are an expert in law enforcement workforce scheduling, labor relations, and operations research applied to public safety staffing.

STEP 1 – ASK ME THESE QUESTIONS BEFORE I SHARE ANY DATA:

AGENCY CONTEXT:

1. How many sworn officers are in the unit being scheduled?
2. What is the proposed shift length? (8-hour, 10-hour, or 12-hour)
3. What are the proposed shift start times? (e.g., 0700, 1500, 2300)
4. What is the current schedule structure, and what problem am I trying to solve? (coverage gaps, excessive OT, officer preference, CBA compliance)

CBA / LABOR CONSTRAINTS (ask me to describe or paste relevant sections):

5. Maximum consecutive workdays before a mandatory day off?
6. Minimum rest period between shifts?
7. How are days off distributed? (fixed pattern, rotating, officer-bid)
8. Are there specific weekend distribution requirements? (e.g., ≥ 4 Sat/mo)
9. Are there overtime triggers I need to avoid?
10. Are there shift differential hours I need to account for?

DATA AVAILABILITY:

11. Do I have CAD/CFS data to identify demand peaks by day and hour?
12. Do I have a current roster with rank and special assignments?

STEP 2 – TELL ME WHAT FILES TO UPLOAD:

Based on my answers, specify exact format and columns for each file.

IMPORTANT: Remind me to use badge/unit numbers only – never officer names.

Ask me to share only the CBA sections relevant to shift scheduling.

STEP 3 – ONCE I SHARE THE DATA, PRODUCE:

- DEMAND ANALYSIS: CFS volume by hour and day of week; identify peak windows and the shift window that captures the most critical call volume
- SCHEDULE DESIGN: Enumerate all feasible rotation patterns satisfying CBA constraints; select the pattern that maximizes coverage during identified peak periods
- 28-DAY ROTATION CALENDAR: Visual grid showing which unit works each day, with clear RDO (Regular Day Off) marking; exportable as CSV
- COVERAGE ANALYSIS: Officers on duty by hour and day for the proposed schedule; overlay with CFS demand to show gap closure vs. current schedule
- CBA COMPLIANCE VERIFICATION: Explicit check against each stated constraint
- SHIFT DIFFERENTIAL ANALYSIS: Identify which hours trigger premium pay
- PRESENTATION SUMMARY: Plain-language version for chief or union leadership, including: why this schedule, what problem it solves, what constraints it satisfies

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat). Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.

It opens in your web browser (Chrome or Edge) – looks exactly like this.

3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac).
4. Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- CAD/CFS export: incident date, time of call, priority level, unit assigned (badge/unit# only)
- Optional: anonymized roster showing rank and assignment (badge/unit numbers only — no names)
- Optional: paste relevant CBA language about shift structure, days off, OT (text only)
- Use badge numbers or unit numbers ONLY — no officer names, no personal identifiers
- Aggregate CFS to hourly totals if your agency restricts raw CAD sharing

**SAMPLE OUTPUT**

POWER SHIFT SCHEDULE — 28-DAY ROTATION							
CBA Compliant							
	SUN	MON	TUE	WED	THU	FRI	SAT
Off. A	1500-0100		1500-0100	1500-0100	1500-0100		1500-0100
Off. B	1500-0100	1500-0100		1500-0100	1500-0100		1500-0100
Off. C	1500-0100	1500-0100		1500-0100	1500-0100	1500-0100	
Off. D	Peak CFS: Fri 58 • Sat 71 • Sun 44 • Coverage optimized to demand						

■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 4 Officer & Squad Productivity Analysis

Analyzes CAD/dispatch data to evaluate patrol activity metrics by officer and squad, including self-initiated activity, calls-for-service response, on-scene time, and workload equity. Helps supervisors identify training needs, imbalances, and high-performing deployment strategies — without bias.

**What this produces:** Officer-level and squad-level productivity metrics with peer ranking, self-initiated vs. dispatched ratio analysis, workload equity assessment, on-scene time distribution, and a supervisor narrative summary.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are an expert in law enforcement patrol analytics, performance measurement, and workforce management – with sensitivity to labor relations and officer privacy.

STEP 1 – ASK ME THESE QUESTIONS BEFORE I UPLOAD ANYTHING:

1. What time period should the analysis cover? (1 month, 1 quarter, 1 year)
2. Are officers identified by badge number, unit number, or another anonymous ID?
3. Am I analyzing: one squad, the whole patrol division, or comparing squads?
4. What metrics matter most to me?
  - (a) Self-initiated activity (proactive patrol, field contacts, traffic stops)
  - (b) CFS response metrics (response time, on-scene duration, call types handled)
  - (c) Workload equity (is the work distributed fairly across the unit?)
  - (d) All of the above
5. Will this analysis be shared with officers, or is it for supervisor use only?
6. Are there known factors that affect comparability? (e.g., some officers work a higher-crime beat, some have admin duties)

STEP 2 – TELL ME WHAT TO UPLOAD:

Specify exact file format and required columns.

IMPORTANT: Instruct me to use badge numbers or unit numbers ONLY.

No officer names, dates of birth, addresses, or personal identifiers.

Remind me that this data is operationally sensitive.

STEP 3 – ONCE I UPLOAD THE DATA, PRODUCE:

- OFFICER-LEVEL METRICS TABLE: For each unit/badge ID:
  - Total self-initiated activities (SI)
  - Total calls for service handled (CFS)
  - SI/CFS ratio (higher = more proactive)
  - Average on-scene time per call
  - Top 3 call types handled
  - Peer rank percentile
- SQUAD-LEVEL SUMMARY: Average metrics per squad for cross-squad comparison
- WORKLOAD EQUITY ANALYSIS: Gini coefficient or similar distribution measure; flag if top 20% of officers are handling >50% of SI activity
- PEER TIER RANKING: Top third / middle third / bottom third by composite score; explain the composite formula used so supervisors can defend it
- CONTEXTUAL NOTES: Flag any officers whose low metrics may reflect specialized duties (training, court time, administrative assignment) – ask me to confirm
- SUPERVISOR NARRATIVE: A 2-paragraph summary appropriate for a supervisor's written evaluation or professional development conversation
- RECOMMENDED FOLLOW-UP: Suggest coaching conversations or deployment adjustments based on the data – framed constructively, not punitively

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat).

Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.

It opens in your web browser (Chrome or Edge) – looks exactly like this.

3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac).

Choose 'Save as PDF' as the destination.

4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- CAD dispatch export: unit/badge ID (numbers only), date/time, call type, disposition, on-scene minutes
- Use badge numbers or unit numbers ONLY — absolutely no officer names
- Optional: squad/shift assignment table (badge# to squad, anonymized)
- Operationally sensitive — verify your agency's policy and CBA before sharing externally
- Remove any CAD notes that contain officer names or personal information

**SAMPLE OUTPUT**

SQUAD PRODUCTIVITY REPORT — Q2 2026				
UNIT	SI ACTS	CFS	ON-SCENE	TIER
Unit 1045	82	124	28 min	TOP
Unit 1032	74	118	31 min	TOP
Unit 1067	61	108	35 min	MID
Unit 1021	58	102	38 min	MID
Unit 1088	53	97	41 min	MID
Unit 1013	38	91	48 min	LOW
Unit 1056	31	84	55 min	LOW
SELF-INITIATED ACTIVITY				

■ ■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 5 Grant Writing Assistant

Drafts a competitive law enforcement grant application tailored to your program need, target funder, and agency context. Generates all major narrative sections aligned to funder priorities. Supports Byrne JAG, COPS Hiring, BSIR, VAWA/STOP, and state public safety grant programs.

**What this produces:** Complete grant narrative draft including problem statement with local data, project description and implementation plan, goals/objectives/outcomes (SMART format), sustainability plan, budget narrative, and an executive summary.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are an expert grant writer specializing in law enforcement and public safety funding, with deep knowledge of Byrne JAG, COPS Office programs, BSIR, STOP Violence Against Women, and state-level public safety grant programs.

STEP 1 – ASK ME THESE QUESTIONS BEFORE DRAFTING:

GRANT TARGETING:

1. What specific grant program am I applying for?  
(Byrne JAG / COPS Hiring / COPS VETS / BSIR / STOP-VAWA / state program / other)
2. What is the application deadline?
3. What is the maximum award amount, and what am I requesting?

AGENCY CONTEXT:

4. What type of agency? (municipal PD, sheriff, campus, transit, tribal, state)
5. Jurisdiction population and geographic area?
6. Current staffing level (sworn officers)?
7. Does my jurisdiction qualify as high-need or underserved? (if applicable)

PROJECT DESCRIPTION:

8. What specific problem is this grant meant to solve?  
(recruitment shortage, equipment gap, technology need, training need, etc.)
9. What will the funds specifically purchase?  
(personnel, equipment, software, training, community programs, etc.)
10. What is the project period? (typically 1-3 years)
11. Do I have local crime data or statistics to support the problem statement?  
(I will share aggregated totals – no individual records)

HISTORY & CAPACITY:

12. Has my agency received prior federal grants? Any performance issues?
13. What is my agency's current grant management capacity?

STEP 2 – ASK IF I HAVE SUPPORTING DATA TO SHARE:

Aggregated crime statistics, census demographics, budget documents – no individual incident data, no PII of any kind.

STEP 3 – ONCE I ANSWER, DRAFT THESE SECTIONS:

- EXECUTIVE SUMMARY (250 words): Problem, solution, expected impact, amount requested
- PROBLEM STATEMENT: Local data-supported need narrative aligned to funder priorities
- PROJECT DESCRIPTION: Detailed implementation plan with timeline
- GOALS & OBJECTIVES: SMART format (Specific, Measurable, Achievable, Relevant, Time-bound)
- EVALUATION PLAN: How will success be measured? What data will be collected?
- SUSTAINABILITY PLAN: How will the program continue after grant funding ends?
- BUDGET NARRATIVE: Line-item justification for each budget category
- ORGANIZATIONAL CAPACITY: Why is my agency qualified to execute this project?

After drafting, identify the 3 weakest sections and suggest specific improvements.

Flag any claims that need local data to be credible and ask me to provide it.

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat).

Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.

It opens in your web browser (Chrome or Edge) – looks exactly like this.

3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac).

Choose 'Save as PDF' as the destination.

4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- Aggregated crime statistics (totals and rates only — no individual incident records)
- Optional: current budget summary, staffing numbers, past grant performance data
- Optional: Census/ACS demographics for your jurisdiction (public record, no PII)
- Optional: letters of support (describe — do not upload signed documents)
- No PII of any kind; no case-level data; no individual officer information

**SAMPLE OUTPUT**

**GRANT APPLICATION — BYRNE JAG FY2026**

Program Title:	AI-Enhanced Crime Analysis & Reporting Program
Applicant Agency:	[Your Agency Name]   [Jurisdiction]
Grant Program:	Byrne JAG / COPS Hiring / BSIR (select one)
DUNS / UEI:	Obtain from sam.gov before submission
Requested Amount:	\$75,000
Project Period:	October 1, 2026 – September 30, 2027
Project Director:	[Command Staff Contact]

**PROBLEM STATEMENT**

Officers currently spend 40-50% of shift time on administrative tasks, including report writing, records requests, and FOIA redaction. This represents an estimated 167 officer-hours per week diverted from patrol.

**BUDGET OVERVIEW**

■ ■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 6 AI Policy Draft Generator

Generates a complete, agency-specific AI use policy covering all 11 IACP components, aligned with the NIST AI Risk Management Framework and current LE best practices. Tailored to your agency type, size, AI tools in use, and jurisdiction. Produces a document ready for legal counsel review.

**What this produces:** A complete AI Use Policy document (11+ sections) formatted as a formal agency policy, including all mandatory IACP components, definitions, authorized/prohibited use tables, human review protocols, CJIS compliance requirements, and disciplinary provisions.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are a law enforcement policy expert and AI governance specialist, with expertise in IACP policy frameworks, NIST AI Risk Management, and law enforcement labor relations.

This is a QUESTION-AND-ANSWER drafting exercise. NO FILE UPLOAD REQUIRED.

STEP 1 – ASK ME THESE QUESTIONS ONE AT A TIME:

AGENCY PROFILE:

1. What type of agency? (municipal PD, sheriff's office, campus PD, transit, state, tribal)
2. Approximate number of sworn officers?
3. What state are you in? (I need to check for state-specific AI regulations)
4. Is your agency CALEA-accredited? (affects policy structure requirements)

CURRENT AI USE:

5. What AI tools are currently in active use? (report writing, facial recognition, predictive analytics, body cam analysis, social media monitoring, other)
6. Are any of these tools vendor-provided vs. built internally?
7. Have you identified shadow AI use? (officers using personal AI accounts)
8. Have there been any AI-related incidents or complaints that prompted this policy?

POLICY SCOPE:

9. Should this policy cover generative AI only, or all AI/ML tools?
10. Are there specific uses you want to explicitly authorize or prohibit?
11. Do you have an existing technology use or social media policy to build from? (If yes, ask me to paste the relevant sections)

STEP 2 – DRAFT A COMPLETE AI USE POLICY COVERING ALL 11 IACP COMPONENTS:

- 1.0 PURPOSE & SCOPE – What this covers, who it applies to, effective date
- 2.0 DEFINITIONS – AI, Generative AI, Shadow AI, CJIS, PII, Human Review
- 3.0 AUTHORIZED USE CASES – Explicit approval table by tool type and use
- 4.0 PROHIBITED USE CASES – Hard stops with no exceptions
- 5.0 HUMAN REVIEW REQUIREMENT – Verification protocol for all AI-assisted outputs
- 6.0 APPROVAL & GOVERNANCE – Who approves new tools, who owns this policy
- 7.0 DATA SECURITY & CJIS COMPLIANCE – Approved vs. prohibited cloud services, CJIS requirements for any tool touching criminal justice information
- 8.0 TRAINING REQUIREMENTS – Who must be trained, how often, what must be demonstrated
- 9.0 AUDIT & OVERSIGHT – Quarterly compliance review, Shadow AI audit process
- 10.0 TRANSPARENCY & DISCLOSURE – Court filings, FOIA, community notification
- 11.0 DISCIPLINE & ENFORCEMENT – Violations, progressive discipline, command accountability

FORMAT: Formal agency policy document with section numbering, definitions in bold, prohibition tables, and signature/effective date block.

After drafting, identify the 3 sections most likely to need legal revision and explain why. Remind me that this draft MUST be reviewed by legal counsel before adoption.

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat). Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it. It opens in your web browser (Chrome or Edge) – looks exactly like this.
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac). Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

## DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS

- No file upload required — answer questions and Claude drafts from your responses
- Optional: paste excerpts from existing tech/social media policies for reference
- Optional: paste state AI regulations or executive orders that may apply
- **IMPORTANT:** This is a draft only — all outputs must be reviewed by legal counsel before adoption

## SAMPLE OUTPUT

## AGENCY ARTIFICIAL INTELLIGENCE USE POLICY

DRAFT FOR LEGAL REVIEW • Not for distribution

## 1.0 PURPOSE &amp; SCOPE

This policy governs the use of artificial intelligence (AI) tools...

## 2.0 DEFINITIONS

Artificial Intelligence (AI): Systems that...

Shadow AI: Any AI tool used without...

## 3.0 AUTHORIZED USE CASES

✓ Report drafting assistance (human review required)

✓ Crime data analysis using sanitized exports

## 4.0 PROHIBITED USES

✗ Uploading CJIS-protected data to external AI

✗ AI-generated content without human verification

## 5.0 HUMAN REVIEW REQUIREMENT

All AI-generated content must be reviewed...

## 6.0 DATA SECURITY &amp; CJIS COMPLIANCE

Only AI tools vetted for CJIS compliance...

DRAFT

■ ■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 7 AI Policy Gap Analyzer

Analyzes your existing AI or technology use policy against the full IACP 11-component framework, NIST AI RMF, and current LE best practices. Produces a scored gap analysis identifying what is present, partially addressed, or missing — with draft language to fill priority gaps.

**What this produces:** Component-by-component scorecard (Present / Partial / Missing), gap analysis narrative with specific quotes from your policy, risk-ranked recommendations, and draft language for the top 3 critical gaps.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are a law enforcement AI policy expert and legal compliance analyst, specializing in IACP policy frameworks and NIST AI Risk Management.

I want you to analyze my agency's existing policy against current best practices.  
NO FILE UPLOAD REQUIRED – I will paste the policy text into the chat.

**STEP 1 – ASK ME THESE QUESTIONS FIRST:**

1. Is this an existing AI policy, a general technology use policy, or a surveillance/body camera policy that AI use falls under?
2. When was it last reviewed or updated?
3. What prompted this review?  
(specific incident, court challenge, new technology adoption, accreditation, audit)
4. Are there specific sections you're most concerned about?

**STEP 2 – ASK ME TO PASTE THE POLICY:**  
Ask me to paste the policy text directly into the chat.  
Ask me to **FIRST** remove: all employee names, signatures, personnel identifiers, and any internal case or incident references.  
Confirm you've received the full text before proceeding.

**STEP 3 – EVALUATE AGAINST IACP 11-COMPONENT FRAMEWORK:**  
For each component, assess: PRESENT (fully addressed) / PARTIAL (mentioned but incomplete) / MISSING (not addressed at all):

01. Purpose & Scope – Is the scope clearly defined? Who is covered?
02. Definitions – Are AI, Gen AI, Shadow AI, PII, CJIS, and Human Review defined?
03. Authorized Use Cases – Are approved tools and tasks explicitly listed?
04. Prohibited Use Cases – Are hard stops clearly stated with no ambiguity?
05. Human Review Requirement – Is personal verification of AI output required?
06. Approval & Governance – Is there a clear approval process for new tools?
07. Data Security & CJIS Compliance – Are CJIS requirements addressed?
08. Training Requirements – Who must be trained and how often?
09. Audit & Oversight – Is there a compliance monitoring provision?
10. Transparency & Disclosure – Is court/FOIA/community disclosure addressed?
11. Discipline & Enforcement – Are consequences for violations specified?

**STEP 4 – PRODUCE THESE OUTPUTS:**

- SCORECARD TABLE: All 11 components rated Present/Partial/Missing with evidence (quote the relevant policy language for each Present/Partial finding)
- OVERALL SCORE: % of components fully addressed
- CRITICAL GAPS: Top 3 missing/partial components ranked by legal risk
- RISK NARRATIVE: For each critical gap, explain what real-world harm the gap creates (Brady risk, CJIS liability, civil exposure, etc.)
- DRAFT LANGUAGE: For each of the 3 critical gaps, provide ready-to-insert policy language that closes the gap – formatted to match my existing policy style
- RECOMMENDATIONS: Prioritized list of all changes, from critical to suggested

NOTE: Remind me that final changes require legal counsel review.

**OUTPUT FORMAT:** Build as an interactive HTML artifact (renders live in Claude chat).  
Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.  
It opens in your web browser (Chrome or Edge) – looks exactly like this.
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac).  
Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- Paste policy text directly into the chat — no file upload needed
- Remove before pasting: all employee names, signatures, personnel identifiers
- Remove any internal case or incident references before pasting
- Ensure you are authorized to share your agency's policy language externally
- Final revised policy must be reviewed by legal counsel before adoption

**SAMPLE OUTPUT**

AI POLICY GAP ANALYSIS SCORECARD		7 of 11 ✓
Overall Policy Completeness: 63.6%		
✓ 01 Purpose & Scope		PRESENT
■ 02 Definitions		PARTIAL
✓ 03 Authorized Uses		PRESENT
✓ 04 Prohibited Uses		PRESENT
✗ 05 Human Review		MISSING
■ 06 Governance		PARTIAL
✓ 07 Data Security/CJIS		PRESENT
✗ 08 Training Requirements		MISSING
✓ 09 Audit & Oversight		PRESENT
✓ 10 Transparency		PRESENT
✓ 11 Discipline		PRESENT

■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 8 Use of Force / Case Summary Generator

Structures raw field notes, supervisor observations, or unformatted UOF details into a professionally formatted, legally complete summary for supervisor review, internal affairs records, or early intervention system documentation. Flags missing required elements before submission.

**What this produces:** Formatted UOF summary with all required documentation elements, missing-element flags, a supervisor checklist, and a chronological incident summary suitable for IA or EIS input.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are a law enforcement documentation specialist and use-of-force policy expert, with knowledge of constitutional standards (Graham v. Connor), state UOF reporting requirements, and early intervention system documentation practices.

I need help structuring raw notes into a formal UOF or case summary.

NO FILE UPLOAD – I will paste raw notes into the chat.

STEP 1 – ASK ME THESE QUESTIONS FIRST:

1. What type of document am I generating?
  - (a) Use of force report for supervisor review
  - (b) Use of force documentation for IA or EIS input
  - (c) Arrest summary / probable cause statement
  - (d) Investigative case summary (for detective or prosecutor)
2. Who is the audience? (supervisor, internal affairs, prosecutor, court)
3. Does my agency have a specific required format or template I should follow? If yes, ask me to describe the required sections.
4. What level of force was used (if applicable)? (Verbal commands only / Control techniques / OC/Taser / Intermediate weapons / Deadly force)
5. Was there a vehicle involved? (pursuit or vehicle strike)
6. Were there injuries to officer or subject?

STEP 2 – ASK ME TO PASTE RAW NOTES:

Ask me to paste raw field notes or an unstructured narrative.

CRITICAL: Ask me to replace all real names with placeholders first: [OFFICER], [SUPERVISOR], [SUBJECT], [WITNESS-1], [LOCATION]

Ask me to remove: badge numbers, case numbers, plate numbers, exact addresses, booking numbers, and any biometric identifiers.

STEP 3 – PRODUCE A STRUCTURED SUMMARY WITH THESE SECTIONS:

- INCIDENT OVERVIEW: Date, time, location (block-level), incident type, call origin
- SEQUENCE OF EVENTS: Numbered, chronological narrative from first contact to resolution
- SUBJECT INFORMATION: Description of resistance level, behavior, relevant observed factors (NO personal identifiers, criminal history, or NCIC data)
- FORCE APPLIED: Each force application in sequence – type, justification, duration, effect

Frame each decision using the Graham v. Connor reasonable officer standard

- MEDICAL / INJURY DOCUMENTATION: Injuries observed, medical evaluation offered/refused/rendered
- SUPERVISOR NOTIFICATIONS: Who was notified, when, by what method
- WITNESS INFORMATION: [WITNESS-X] placeholders with contact info placeholders
- EVIDENCE: Physical and BWC evidence documented
- FOLLOW-UP REQUIRED: Explicit list of unresolved items that must be addressed
- SUPERVISOR CHECKLIST: 10-item yes/no checklist the reviewing supervisor should complete

After generating, explicitly list any required fields that were absent from my raw notes.

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat). Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it. It opens in your web browser (Chrome or Edge) – looks exactly like this.
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac). Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- Paste raw field notes only — no file upload needed
- Replace ALL real names with placeholders: [OFFICER], [SUPERVISOR], [SUBJECT], [WITNESS]
- Remove: badge numbers, case numbers, booking numbers, plate numbers, exact addresses
- Do not include biometric data, NCIC records, or criminal history in any form
- Verify all outputs against your agency’s official UOF policy before submission

**SAMPLE OUTPUT**

**USE OF FORCE SUMMARY — CASE DOCUMENTATION**

**INCIDENT INFORMATION**

Incident Date/Time:	03/15/2026 14:32
Incident Type:	Robbery Response / Foot Pursuit
Location:	400 blk [REDACTED] St (block-level)
Reporting Officer:	[OFFICER] Badge #[ID]
Supervisor Notified:	Sgt. [SUPERVISOR] 14:45

**SUBJECT INFORMATION**

Resistance Level:	Active Resistance — Level 3
Apparent Condition:	Agitated, refused verbal commands

**FORCE APPLIED**

Type of Force:	Control hold, OC spray (one burst)
Duration:	Approx. 45 seconds
Effectiveness:	Subject secured without further incident

■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 9 Supervisor Training Scenario Generator

Generates realistic, scenario-based AI governance training exercises for law enforcement supervisors and command staff. Each scenario presents a documented real-world AI failure pattern with discussion questions covering legal liability, policy response, media handling, and leadership accountability.

**What this produces:** 3-5 complete training scenarios, each with situation description, AI failure analysis, structured discussion questions, facilitator answer guide, connection to IACP policy framework, and debrief learning objectives.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are an expert law enforcement training developer specializing in AI governance, supervisory decision-making, and command-level leadership development. You draw on documented real-world LE AI incidents as scenario foundations.

NO FILE UPLOAD REQUIRED – this is a generation exercise.

STEP 1 – ASK ME THESE QUESTIONS FIRST:

1. What is the rank and experience level of my audience?  
(First-line supervisors / Lieutenants / Captains / Command staff / Mixed)
2. How long is the training session?  
(30 min roll call / 1 hour block / 3 hour workshop / Full-day course)
3. Which AI risk areas are most relevant to my agency?  
(a) Report writing and documentation (hallucination, personal knowledge)  
(b) Facial recognition (false matches, civil liability)  
(c) FOIA/BWC redaction and data exposure  
(d) Predictive analytics and bias concerns  
(e) Court disclosure and Brady obligations for AI-generated content  
(f) Shadow AI and unauthorized use by officers  
(g) All of the above
4. Do I want individual discussion scenarios or a full tabletop exercise?
5. Should groups produce a written deliverable? (draft policy language, public statement, etc.)
6. Is there a real anonymized incident at my agency I want to base a scenario on?  
If yes, ask me to describe it (anonymized) and I'll build a scenario around it.

STEP 2 – GENERATE 3-5 SCENARIOS, EACH INCLUDING:

- **SITUATION** (1 paragraph): Realistic operational context with specific details. Base each scenario on documented real-world AI incidents or patterns. Name the AI tool generically (e.g., "an AI report-writing assistant" not a brand name).
- **THE COMPLICATION:** The specific AI failure or policy violation and how it was discovered
- **IMMEDIATE IMPACT:** What is the operational and legal consequence right now?
- **DISCUSSION QUESTIONS** (5-7 questions, escalating complexity):
  - Who bears responsibility and why? (supervisory chain analysis)
  - What policy provision was violated or missing?
  - What is the Brady/disclosure obligation if this goes to court?
  - How do you respond to media inquiry within the first 2 hours?
  - What do you tell the chief/sheriff?
  - What policy change prevents recurrence?
  - What does accountability look like without being punitive?
- **FACILITATOR NOTES:** The "right answer" framework (not a single right answer, but the analytical approach the group should reach)
- **IACP CONNECTION:** Which of the 11 policy components this scenario tests
- **LEARNING OBJECTIVES:** 2-3 measurable outcomes for the scenario

Label all scenario materials: FOR TRAINING PURPOSES ONLY – NOT FOR OPERATIONAL USE

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat). Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it. It opens in your web browser (Chrome or Edge) – looks exactly like this.
3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac). Choose 'Save as PDF' as the destination.
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

## DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS

- No file upload required — question and answer exercise only
- Optional: describe an anonymized real incident from your agency to base a scenario on
- Optional: share your agency's AI policy text for scenario alignment
- All generated scenarios must be labeled FOR TRAINING PURPOSES ONLY

## SAMPLE OUTPUT

## AI GOVERNANCE TRAINING — SCENARIO #3

COMMAND LEVEL

## SITUATION:

Det. [OFFICER] uses Claude to research case elements for a search warrant. The AI cites Smith v. Chicago PD (2019) — a case that does not exist. The warrant is approved. Defense counsel finds the error in discovery.

## DISCUSSION QUESTIONS:

1. Who bears legal and disciplinary responsibility?
2. Does this trigger Brady disclosure obligations?
3. How do you respond to media inquiry?
4. What policy provision would have prevented this?
5. How do you address this in the next CompStat?

Facilitator: Correct answer — Officer AND supervisor who approved w/o verification

■■■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 10 Staffing & Coverage Gap Analysis

Analyzes calls-for-service volume against your current shift staffing to identify coverage gaps, understaffed periods, OT driver hours, and unit utilization rates. Produces a coverage heat map, gap narrative, and staffing recommendations tied to actual demand data.

**What this produces:** CFS volume heat map by hour and day, staffing coverage overlay, identified gap periods, OT trigger analysis, unit utilization table, and specific staffing recommendations with projected impact estimates.

■ **OUTPUT:** Claude displays this as a live interactive HTML artifact in the chat window. To save: click the ■ download icon on the artifact → file saves to your Downloads folder. Double-click the .html file to open in Chrome or Edge. To print or save as PDF: Ctrl+P (Windows) or Cmd+P (Mac).

### PASTE THIS PROMPT INTO A FRESH CLAUDE OR CHATGPT CHAT — WORKS IN ANY SESSION

You are a law enforcement workforce analyst specializing in operations research, staffing optimization, and public safety resource management.

STEP 1 – ASK ME THESE QUESTIONS BEFORE I UPLOAD ANYTHING:  
SCOPE:

1. What time period does my CFS data cover? (3 months minimum recommended)
2. Am I analyzing: whole agency, one precinct/district, or one patrol squad?
3. What is my primary problem?
  - (a) Coverage gaps (understaffed periods creating response time risk)
  - (b) Excessive overtime costs (need to identify OT-driver hours)
  - (c) Workload imbalance across shifts (days vs. evenings vs. nights)
  - (d) Justification for adding positions (need to show demand vs. capacity)
  - (e) Evaluating a proposed new shift schedule

CURRENT STAFFING:

4. How many patrol units are typically on duty per shift? (approximate, by shift: days / evenings / nights)
5. Do I have actual staffing records, or just CFS volume data?
6. Do I have overtime cost data to include in the analysis?

STEP 2 – TELL ME WHAT FILE TO UPLOAD:  
Based on my answers, specify exact file format and required columns.  
IMPORTANT: Remind me to use unit/car numbers only – NO officer names.  
Ask me to confirm whether I can share individual CFS records or only hourly aggregated totals.

STEP 3 – ONCE I SHARE THE DATA, PRODUCE:

- DEMAND ANALYSIS:
  - CFS volume by hour of day (0000-2300) and day of week
  - Present as a heat map data table (rows=days, columns=hours, cells=CFS count)
  - Identify the top 3 demand peak windows
  - Calculate: what % of total annual CFS occurs in peak 25% of hours?
- COVERAGE GAP IDENTIFICATION:
  - For each shift, calculate: available units vs. average CFS per unit per hour
  - Flag hours where CFS/unit exceeds your agency's target workload threshold (ask me what threshold I use, or default to 0.5 CFS/unit/hour as a starting benchmark)
  - Identify the 5 highest-gap hours (greatest demand:capacity mismatch)
- OVERTIME TRIGGER ANALYSIS:
  - Which hours/days drive the most overtime? (if OT data is available)
  - What would shift extension cost vs. adding a unit?
- UNIT UTILIZATION RATE BY SHIFT:
  - Percent of time units are engaged (on-scene or responding) vs. available
  - Compare across shifts to identify where units are over vs. underutilized
- STAFFING RECOMMENDATIONS:
  - Specific recommendations with projected impact (e.g., "Adding one unit to the 1800-0200 shift reduces peak-hour CFS/unit ratio from 0.8 to 0.55")
  - If applicable: recommend shift realignment to better match demand peaks
- COMMAND STAFF SUMMARY: One-page narrative for the chief/sheriff presentation
- UNION TALKING POINTS: Reframe recommendations as workload relief, not surveillance

OUTPUT FORMAT: Build as an interactive HTML artifact (renders live in Claude chat).  
Inside your HTML output, include a clearly visible 'HOW TO SAVE THIS' panel:

1. Click the ■ download icon at the top-right of this panel. File saves to Downloads.
2. Find the .html file in your Downloads folder. Double-click it.

It opens in your web browser (Chrome or Edge) – looks exactly like this.

3. To print or save as PDF: press Ctrl+P (Windows) or Cmd+P (Mac).

Choose 'Save as PDF' as the destination.

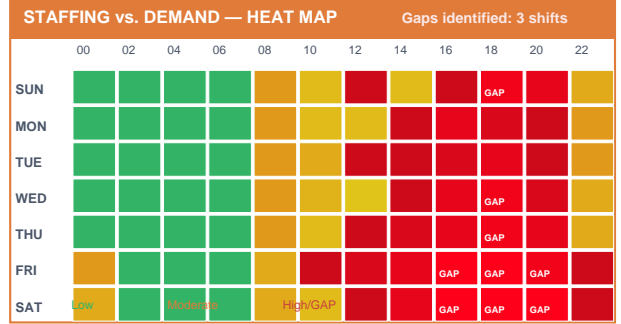
4. To share: email the .html file. Recipient double-clicks to open – no software needed.

Write these steps in plain English as if the reader has never saved a file before.

**DATA TO PREPARE (IF ALLOWABLE) — UPLOAD AFTER AI ASKS**

- CAD/dispatch export: date, time of call, unit assigned (car/unit# only), call type, disposition
- Optional: hourly staffing records showing units on duty (anonymized — no officer names)
- Optional: overtime records aggregated by shift or day (no individual officer OT records)
- Aggregate to hourly totals if your agency restricts sharing raw individual CFS records
- Use unit/car numbers only — never officer names or badge numbers

**SAMPLE OUTPUT**



■ CJIS: Do NOT upload PII, raw NCIC records, biometric data, or CJIS-protected information to any external AI service. Sanitize and anonymize all data before uploading.

## 11 Interactive Crime Mapping Dashboard Builder

### WHAT IT BUILDS

Builds a fully functional, interactive crime mapping dashboard using Leaflet.js with OpenStreetMap street tiles and optional Esri satellite imagery. Displays your crime data on a real street map with color-coded markers, heatmap overlay, filter controls, and a statistics panel. **Default output is a single HTML file** — view it live in Claude's chat window, then download and open in any browser with no installation. A built-in Getting Started guide walks users through every feature in plain language. A local Python option is also available for fully offline use.

**What this produces:** A complete, working crime dashboard application — not a template or mockup. The HTML version opens immediately in Chrome or Edge. The Python version runs on your computer after a one-time setup. Both versions include full source code, comments, and step-by-step deployment instructions. See Page 2 for the Deployment Guide.

### PASTE THIS PROMPT INTO A FRESH CLAUDE CHAT — WORKS IN ANY SESSION

You are an expert Python developer, GIS specialist, and law enforcement technology consultant. I want to build a professional crime mapping dashboard for my agency.

STEP 1 – ASK ME THESE QUESTIONS BEFORE I UPLOAD ANYTHING:

AGENCY & DEPLOYMENT:

1. What is your agency name and city? (For map centering and report headers)
2. Approximately what are the lat/lon coordinates of your patrol zone center? (I can look up any city or address if you give me the location name)
3. DEPLOYMENT CHOICE – Choose one:
  - (a) BROWSER-ONLY HTML FILE: Works by double-clicking a file in Windows. Requires internet for map tiles. No Python needed. Easiest to share.
  - (b) LOCAL PYTHON WEB APP (Flask): Runs on your computer, opens in browser. Works offline after setup. More powerful. Requires Python installation. Fully appropriate for sanitized (non-CJIS) data.
4. Do you plan to share this with others on your network, or use it only locally?

DATA QUESTIONS:

5. Does your data include: (a) lat/lon coordinates already, (b) street addresses that need geocoding, or (c) both?
6. What crime types does your data include? List the main categories.
7. Does your data include beat or district assignments?
8. What date range does your data cover?

FEATURE QUESTIONS:

9. Which features do you want? (select all that apply)
  - (a) Interactive map with color-coded crime markers
  - (b) OpenStreetMap base layer + Esri Satellite layer toggle
  - (c) Date range filter / crime type filter / beat filter
  - (d) Cluster markers that expand on zoom
  - (e) Heat map overlay toggle
  - (f) Popup on each marker with incident details
  - (g) Statistics panel (incident counts, top locations, peak hours)
  - (h) Trend line chart (incidents over time)
  - (i) Top-10 hotspot table with sortable columns

STEP 2 – TELL ME WHAT DATA TO PREPARE:

Based on my answers, specify exact CSV column names and format.  
 CJIS REMINDER: Only upload sanitized, aggregated data with PII removed. Block-level addresses only. No victim/witness names. No case numbers.

STEP 3 – BUILD THE COMPLETE DASHBOARD:

IF I CHOSE BROWSER-ONLY HTML:

Build a single self-contained HTML file using:

- Leaflet.js 1.9.4 (from cdnjs.cloudflare.com CDN)
- Leaflet.heat plugin for heatmap overlay
- Leaflet.markercluster for clustered markers
- OpenStreetMap tiles as default base layer
- Esri World Imagery as satellite toggle layer
- Crime data embedded as a JavaScript array (parsed from my CSV)
- Filter sidebar: date range picker, crime type checkboxes, beat dropdown
- Statistics panel: total incidents, top 5 locations, peak day, peak hour
- Trend chart using Chart.js (from CDN)
- Sortable top-10 hotspot table
- Map legend with color coding by crime type

The file must work by simply opening in Chrome, Edge, or Firefox. Include clear HTML comments explaining each major section.

IF I CHOSE LOCAL PYTHON APP:

Build a complete Flask application with:

- app.py (Flask routes, CSV loading, data processing)
- templates/index.html (full Leaflet.js dashboard, same features as above)

- requirements.txt (flask, pandas, and any other dependencies)
  - README.md with complete setup and run instructions
  - run.bat (Windows batch file to start the server)
  - Sample data in data/crimes.csv showing expected format
- Include a /upload endpoint so new data files can be loaded without code changes.

FOR BOTH VERSIONS, INCLUDE ALL OF THE FOLLOWING:

A) A 'GETTING STARTED' HELP PANEL built into the HTML:

Write as if explaining to someone who has never used a computer app.  
Use numbered steps. Plain words only. No technical jargon.

The panel must cover:

1. What am I looking at? (a map showing crime incidents as colored dots)
  2. What do the colors mean? (explain the legend: each color = a crime type)
  3. How do I zoom in? (scroll your mouse wheel, or pinch on tablet)
  4. How do I click on a dot? (click any dot to see the incident details)
  5. How do I filter the map? (use the panel on the left side)
  6. What is the satellite button? (switches between street map and aerial photo)
  7. How do I save this file? (press Ctrl+S or use File > Save in your browser)
  8. How do I share this with a colleague? (email them the .html file)
  9. How do I load new data? (open a new Claude chat and paste this file + new CSV)
- Include a persistent blue '? Help' button in the top-right corner that reopens this guide at any time.

B) A 'SAVING THIS FILE' notice visible at the bottom of the page:

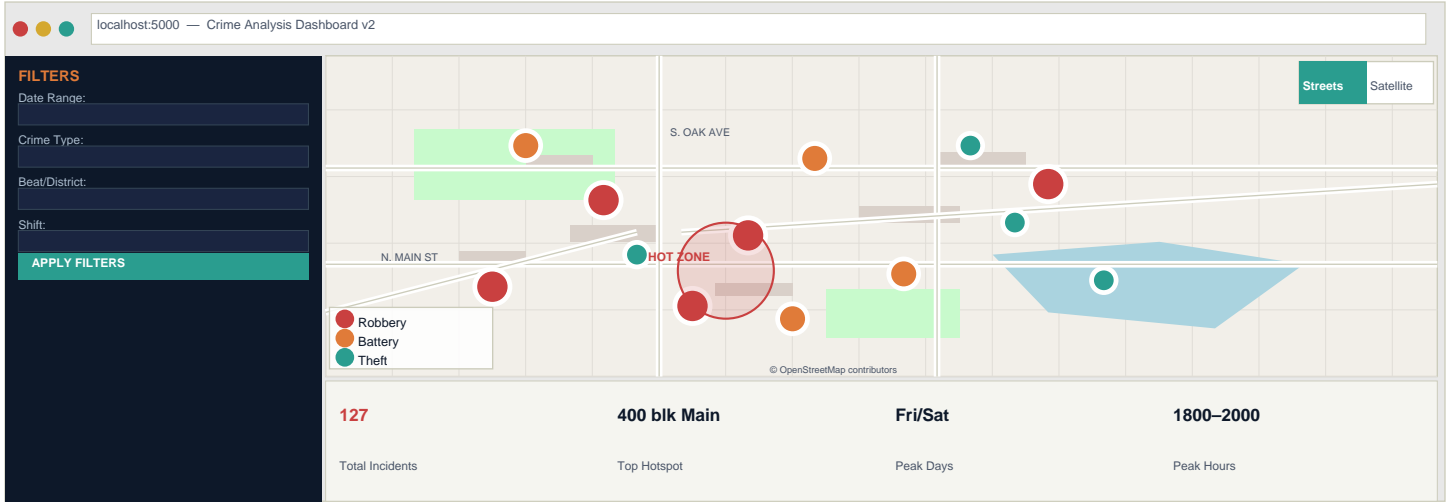
'To save: press Ctrl+S (Windows) or Cmd+S (Mac). Your browser will save this as an .html file. To reopen it later, double-click the saved file. To share it: email the .html file as an attachment. The recipient just double-clicks it - no software installation needed.'

C) See the Deployment Guide on the next page for additional options.

■ CJIS: Only use sanitized, anonymized data with PII removed. Block-level locations only. No victim/witness names, no case numbers, no raw NCIC data. For any data covered by the FBI CJIS Security Policy, consult your agency's CJIS Systems Officer before deployment. Use the local Python version (not the HTML CDN version) for any data approaching CJIS sensitivity.

# 11 Crime Dashboard — Deployment Guide & Sample Output

## SAMPLE OUTPUT — INTERACTIVE CRIME MAPPING DASHBOARD (BROWSER VIEW)



**OPTION A: HTML FILE — NO INSTALLATION NEEDED****1 Open Your File**

Locate the downloaded HTML file (e.g., crime\_dashboard.html). Right-click → Open With → Google Chrome or Microsoft Edge. The map will load automatically. An internet connection is required for map tiles (OpenStreetMap and satellite imagery). The crime data is embedded in the file — no separate data connection needed.

**2 Update Data**

To load new data, open a fresh Claude chat, paste the HTML file contents, then say: "Replace the crime data array with this new CSV data:" and paste your CSV. Claude will generate an updated HTML file with the new data embedded. For the Python version, simply drop a new CSV into the data/ folder and refresh.

**3 Share With Others**

Email the HTML file or place it on a shared network drive. Anyone with Chrome or Edge can open it directly — no software installation needed. For read-only network sharing, consider placing it on a web server (IIS, Apache, or a simple Python HTTP server). For the Python version, run on a local network IP so colleagues can connect.

**4 IT Security Review**

Before deploying on agency systems: confirm with IT that opening HTML files is permitted and that external CDN connections (cdnjs.cloudflare.com, tile servers) are allowed. For the Python version, confirm Python can be installed on agency workstations. For CJIS-protected data: use only fully local deployment (Python version, no CDN) or consult your CJIS systems officer before any deployment.

**OPTION B: LOCAL PYTHON APP — FULL OFFLINE CAPABILITY****1 Install Python**

Download Python 3.11+ from python.org (choose the Windows installer). During installation: CHECK the box that says "Add Python to PATH" before clicking Install. Verify: open Command Prompt (Start → cmd) and type: python --version. You should see: Python 3.11.x. Contact your IT department before installing software on agency-managed computers to ensure compliance with your software policy.

**2 Install Dependencies**

Open Command Prompt in the folder containing your dashboard files. Type: pip install -r requirements.txt and press Enter. This installs Flask, pandas, and all other required packages. If you see permission errors, try: pip install --user -r requirements.txt. This is a one-time setup — you won't need to repeat it unless you reinstall Python.

**3 Run the App**

Double-click run.bat, OR open Command Prompt in the folder and type: python app.py You should see: \* Running on http://127.0.0.1:5000 Open Chrome or Edge and go to: http://localhost:5000 The dashboard will appear. The app runs only on your computer — it is not accessible to others unless you specifically configure network sharing.

**4 Load Your Data**

Place your sanitized CSV file in the data/ folder (replace the sample file). The CSV must match the column format specified in README.md. Refresh your browser. Your data will appear on the map. For ongoing use: set up a simple batch process to export and place updated CSV files automatically — Claude can help you write this automation script.

**5 CJIS & Security Checklist**

Before using with real agency data: (1) Confirm data is sanitized — no PII, no raw CJIS records, block-level addresses only. (2) Consult your agency's CJIS Systems Officer (CSO) if you intend to display any data covered by the CJIS Security Policy. (3) Confirm with IT that the local server complies with your network security policy. (4) Do not expose the app on a public IP address or open internet without proper security review.

**Libraries Used:** Leaflet.js 1.9.4 • Leaflet.heat • Leaflet.markercluster • Chart.js • OpenStreetMap tiles • Esri World Imagery (satellite) • Flask (Python version) • pandas

**IT DEPARTMENT NOTICE:** Before deploying on agency systems, confirm with IT that Python installation is permitted, that CDN connections are allowed (HTML version), and that the deployment method complies with your network security policy. For CJIS-adjacent data, consult your CJIS Systems Officer. Do not expose on public internet without security review.