Visualizing Truth

Advanced Data Visualization for Investigators: How to turn complex data into a clear, persuasive, and undeniable narrative.

The Challenge: The Limits of Text

In arbitration or executive briefings, dense reports and spreadsheets fail to convey complex relationships. Visual evidence is processed faster and is far more persuasive.

60,000X

Faster the human brain processes images compared to text.

43%

More persuasive a presentation becomes when visuals are used to support key arguments.

Three Essential Visualizations for Complex Cases

These three advanced techniques transform raw data into compelling visual narratives that are easy for non-technical audiences to understand.

Link Analysis Graph

Shows the hidden relationships between people, organizations, and assets. Perfect for uncovering conspiracies.

Sankey Diagram

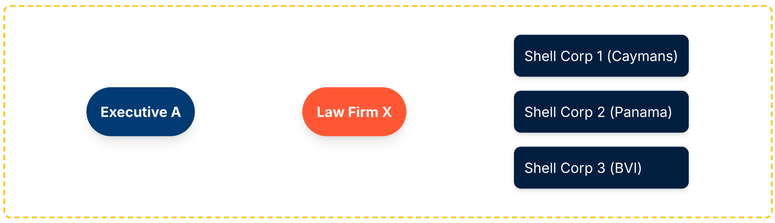
Visualizes the flow of money, data, or resources from a source to a destination. Ideal for financial crimes.

Heatmap

Displays activity density over time, instantly revealing patterns, anomalies, and outliers in logs or timelines.

Example: Uncovering a Shell Corporation Network

A Link Analysis Graph instantly shows what a spreadsheet cannot: the central role a single law firm plays in connecting a corrupt executive to a series of offshore shell corporations.

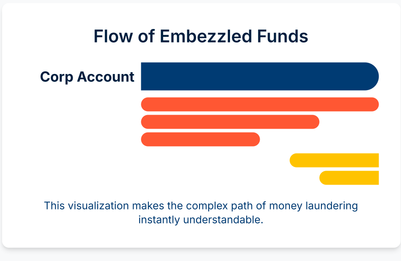


This visual immediately identifies "Law Firm X" as the central node requiring further investigation.

Example: Following the Money

A Sankey Diagram (approximated here with a flow chart) visually demonstrates how embezzled funds were moved. It clearly shows the initial source of the funds, the intermediary accounts used for laundering, and the final destinations.

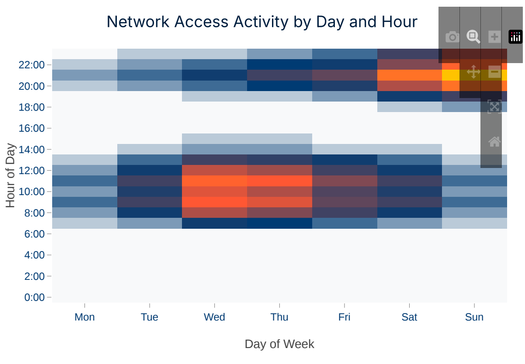
- **Source: Corp Account**
- **Laundering: 3 Shell Corps**
- **Destination: Personal Assets**



This visualization makes the complex path of money laundering instantly understandable.

Example: Identifying Anomalous Activity

A Heatmap is the best way to analyze thousands of log entries to find a pattern. In this example, network access logs immediately reveal an employee was accessing sensitive files at highly unusual times—late at night and on weekends.



The bright yellow squares clearly indicate a high concentration of activity during non-business hours, pinpointing the exact time frame for the data breach.

Infographic generated from Knowledge Article KA-RP-706. This visualization does not use Mermaid JS or SVG graphics.