MOSCOW FORENSICS DAY ‘25



NIKITA PAVLOV

“THE ROLE OF THE USER INTERFACE IN DIGITAL INVESTIGATIONS: HOW UI CONVENIENCE AND INTUITIVENESS SPEED UP DATA ANALYSIS AND SEARCH?”

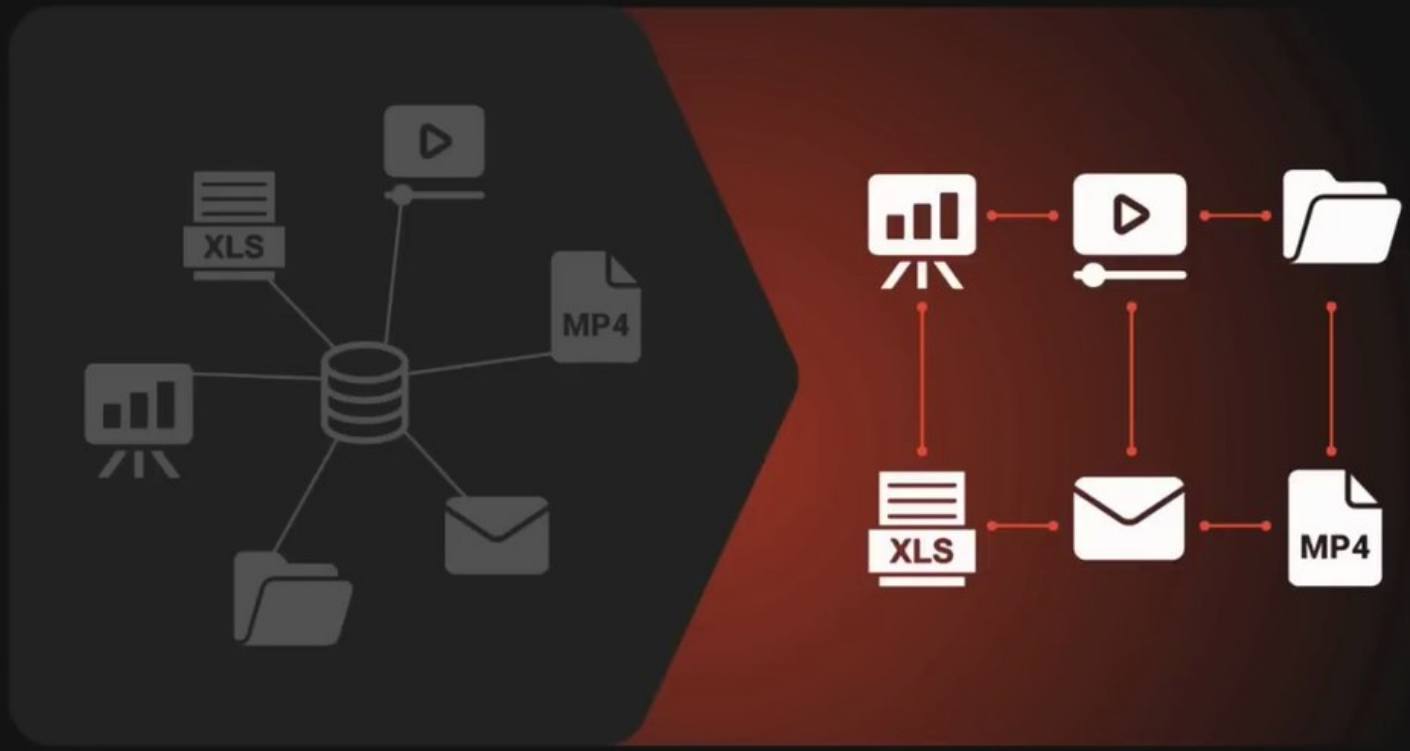
FORENSIC DATA ANALYSIS LABORATORY LLC

MFD

Problem: “Information overload”

Hick's law: “The more choices, the longer the decision”

Decision time grows with the number and options of choice. complexity



UI/UX — not about “pretty”, but about “effective”

UI (User Interface) — buttons, menus, colors, fonts. The outer layer.



UX (User Experience) — feelings, ease of reaching the goal, logic of work. The inner essence.

Goal: make the tool help you think about the investigation, not about how to use it.





Cognitive load

Our brain has a limited “RAM”

We can hold 7±2 items of information in our head at once.

A complex interface “clogs” this memory with routine (“where's that button?”, “how to filter here?”).

UI goal: cut the load by taking on routine tasks.
Free brain resources — for analysis and decision-making.

Visual perception (Gestalt principles): Eye and brain love order

Proximity principle

Elements placed next to each other are perceived as related.

Similarity principle

Elements of the same color, shape or size are perceived as a group.

Closure principle

In visualization tools (relationship graphs) a group of interacting objects is outlined by a barely visible semi-transparent area (a contour), even if the line is not solid.

Common fate principle

Elements that move in the same direction or appear/disappear at the same time are perceived as related.

Figure and ground principle

A pop-up warning window dims the background under it, clearly separating itself as the “figure”. A high-priority log line has a contrasting background color to stand out clearly from the other lines (the “ground”).

Application

Correct grouping of buttons

use of color to highlight anomalies (red — threat, green — normal).

Case: Investigating a phishing incident

UI as a reaction accelerator

Saves 20-30 minutes on every incident.

09:00: A complaint comes in from a user.
09:02 (Bad UI): Analyst manually hunts the email in mail server logs via a complex query. Spends 15-30 minutes.

09:02 (Good UI): Enters the sender's email into the unified search box. The system finds it in 10 sec. and shows all recipients and attachments.
09:10 (Good UI): Click on the attachment hash.
09:12 (Good UI): “Block sender” button + “Find all occurrences”. The system runs and shows the result.

09:20: Incident contained, emails deleted, users warned.



What to demand from developers? Practical tips

Unified search

One window for all data types

Hotkeys

For frequent actions

Templates and dashboards

Ability to tailor views to the task.

Clarity and unambiguity

No techie terms on buttons

Relationship visualization

Graphs and maps, not just tables.

Feedback

The system must report on actions (“Searching...”, “Done”).

Formulate and voice your requirements for the interfaces of the tools you use.

Business benefits

A convenient interface is not a cost, it's an investment



Speed: Faster response → smaller losses.

Accuracy: Fewer errors from the human factor.

Efficiency: One analyst can process more information.

Satisfaction: Less burnout, retention of valuable staff.

Summary



UI/UX — a critically important component of investigation tools.



A good interface reduces cognitive load and saves time, based on the laws of perception.



Your job — not to put up with inconvenient systems, but to advocate convenience and efficiency.

Questions

Никита Павлов

inbox@zero-ediscovery.ru

zero-ediscovery.ru

zero-ediscovery.ru

@zero_ediscovery