Digital Evidence Programme

Evidence Analysis and Review: Characterisations of Current and Target System Architectures

Andy Bidmead, Programme Lead

Iain Nicoll, Business Architect

28/02/2023

POLICE DIGITAL SERVICE

Challenge area: victim and witness experience

Better tools to allow the victim to make their case using data.

Using selective extraction to only have data that the officer needs to use for the case.

Returning handsets quicker – aided by swifter analysis.

Looking at the end-to-end process for rape investigations.

Challenge areas: how case data is used, analysed and presented

Common standards for digital, data and tech use for cases.

Tech designed to meet the challenges of investigating RASSO.

Development of tools and widening the market for solutions.

Reducing the need for manual tasks and interpreting data.

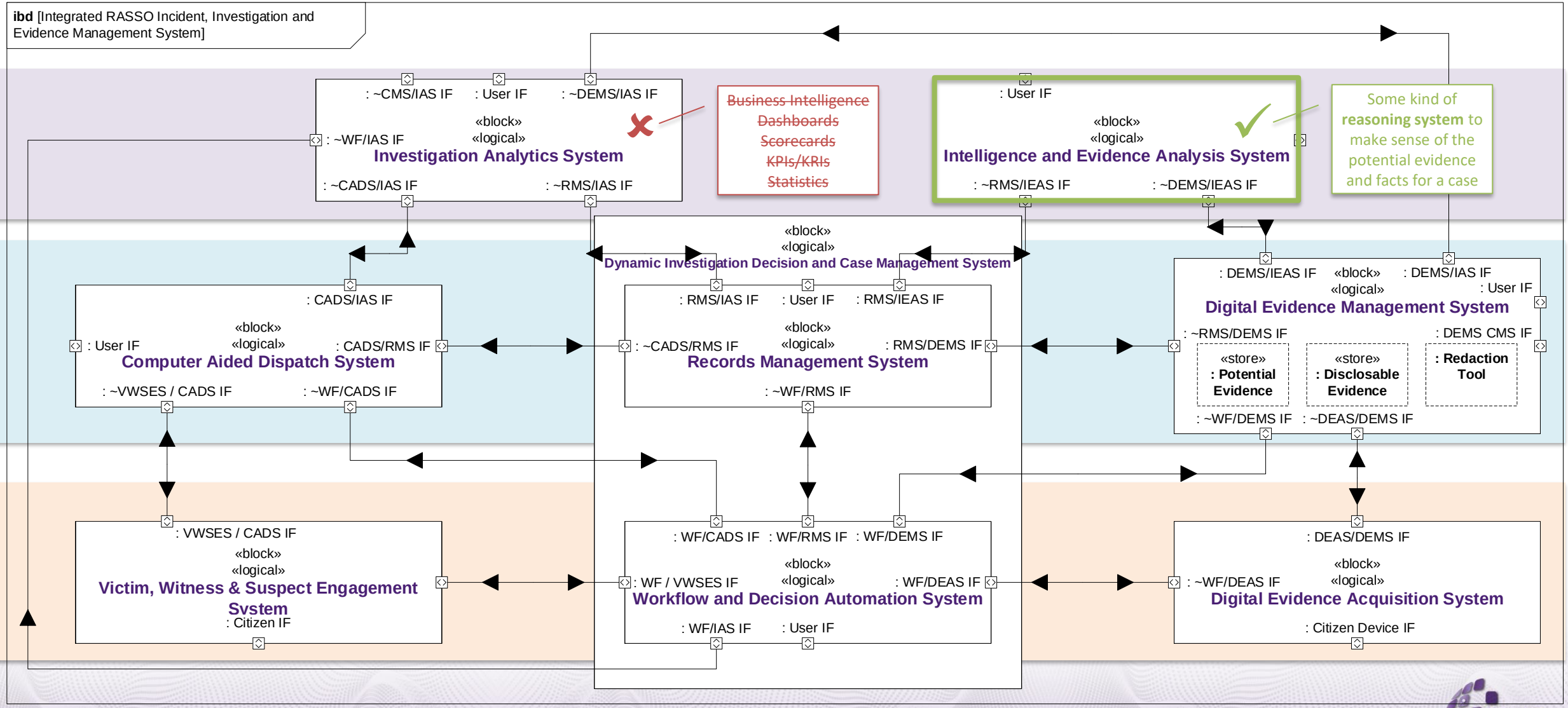
Testing, proving and validating solution design.

Increasing the use of automation to improve efficiency.

Problem / opportunity statement

Who are the users of any prospective solution?	Police RASSO investigators and analysts as support staff The vision would be to make the analysis of evidence as easy as possible for **investigators** to conduct, rather than having to rely on (and often wait for) analyst support
What is the challenge?	• Huge volumes of sensitive data on phones & cloud platforms • Digital evidence in various media combined with multiple other data sources • Limited tools for reviewing data in multiple formats • Time consuming trawling through information in disparate data stores
Where does the source information come from?	Police force systems of record (RMS, DEMS, CAD). These will remain – we are not looking to replace these but to better use the information recorded in these systems. As a next step we may also wish to bring in information from police intelligence systems, if practicable to do so.
How should the information be presented to the user?	A timeline of events before, during and after the reported incident(s), with events underpinned by items of evidence

Analysis and review in the context of our top-level system architecture



Definitions of key terms

analysis
systematic examination in which the biological or technical system is decomposed into its component parts using suitable methods, after which the parts are then organized and evaluated. The opposite of analysis, in terms of its aspect of “resolution into individual parts”, is referred to as synthesis (recomposition)
[ISO 18458:2015]

evaluation of potential digital evidence in order to assess its relevance to the investigation. Potential digital evidence, which is determined as having relevance, becomes digital evidence
[ISO/IEC 27042:2015]

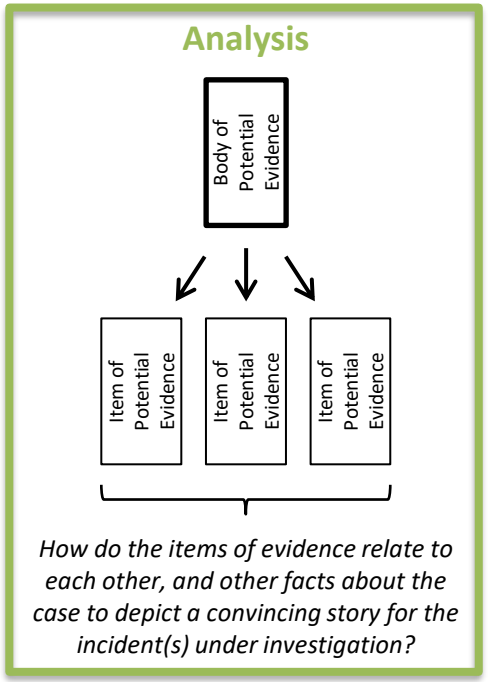
reasoning
process by which a person or a computer performs analysis, classification or diagnosis, makes assumptions, solves problems, or draws inferences
[ISO/IEC 2382:2015]

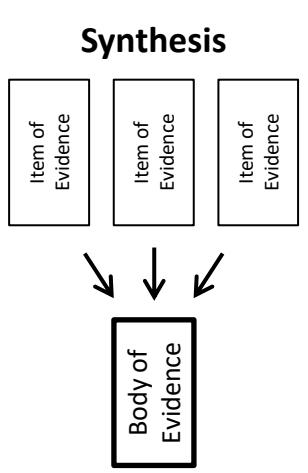
review
determination of the suitability, adequacy or effectiveness of an object to achieve established objectives
[ISO 9000:2015]

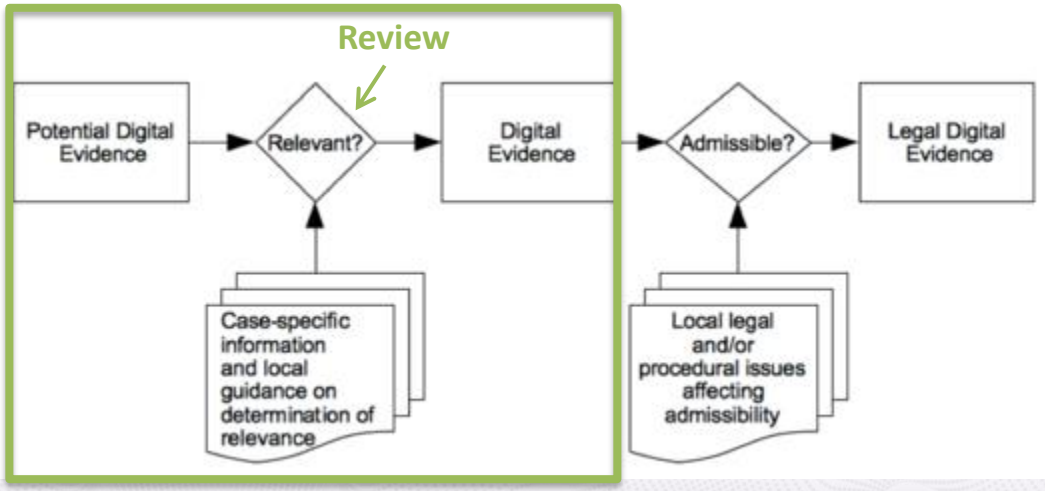
digital evidence
information or data, stored or transmitted in binary form which has been determined, through the process of analysis, to be relevant to the investigation
[ISO/IEC 27042:2015]

potential digital evidence
information or data, stored, or transmitted in binary form which has not yet been determined, through the process of analysis, to be relevant to the investigation
[ISO/IEC 27042:2015]

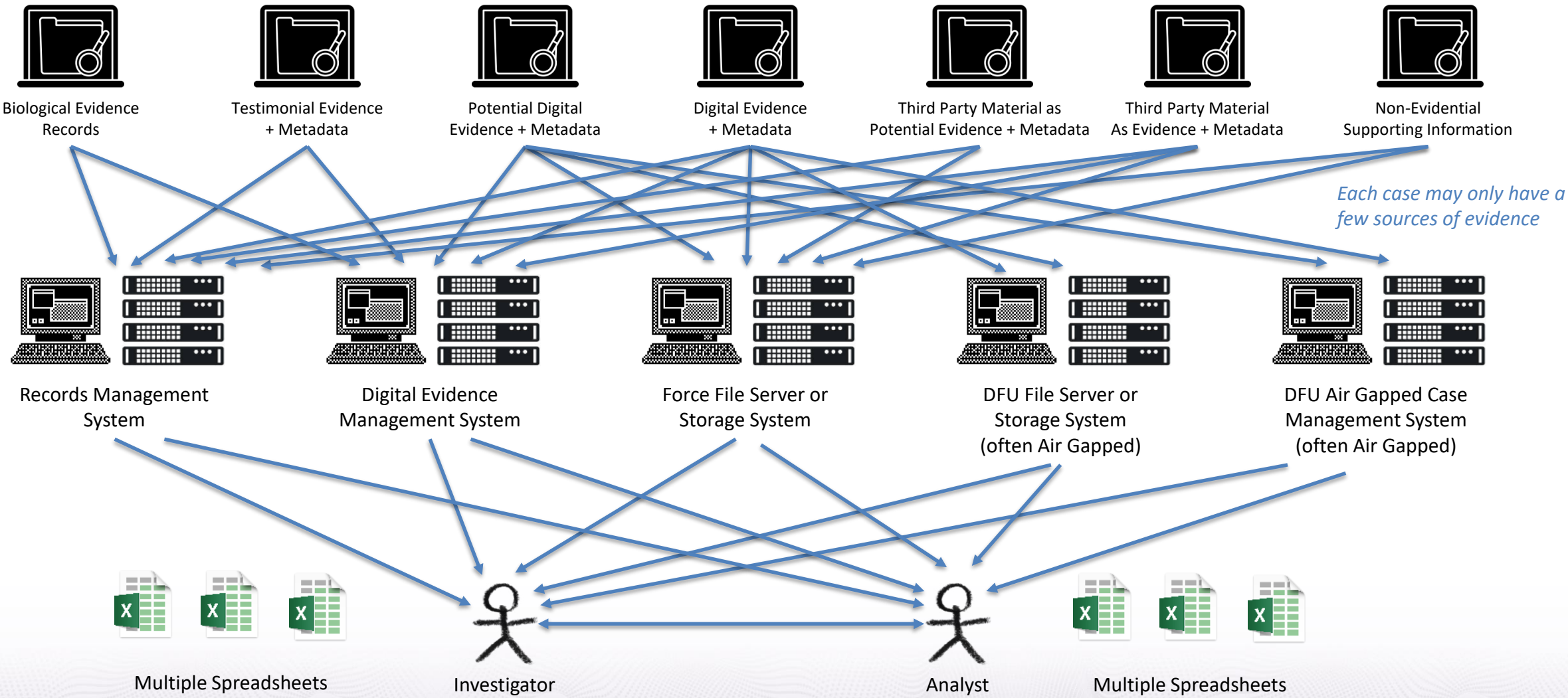
legal digital evidence
digital evidence which has been accepted into a judicial process
[ISO/IEC 27042:2015]







Characterisation of current system architecture

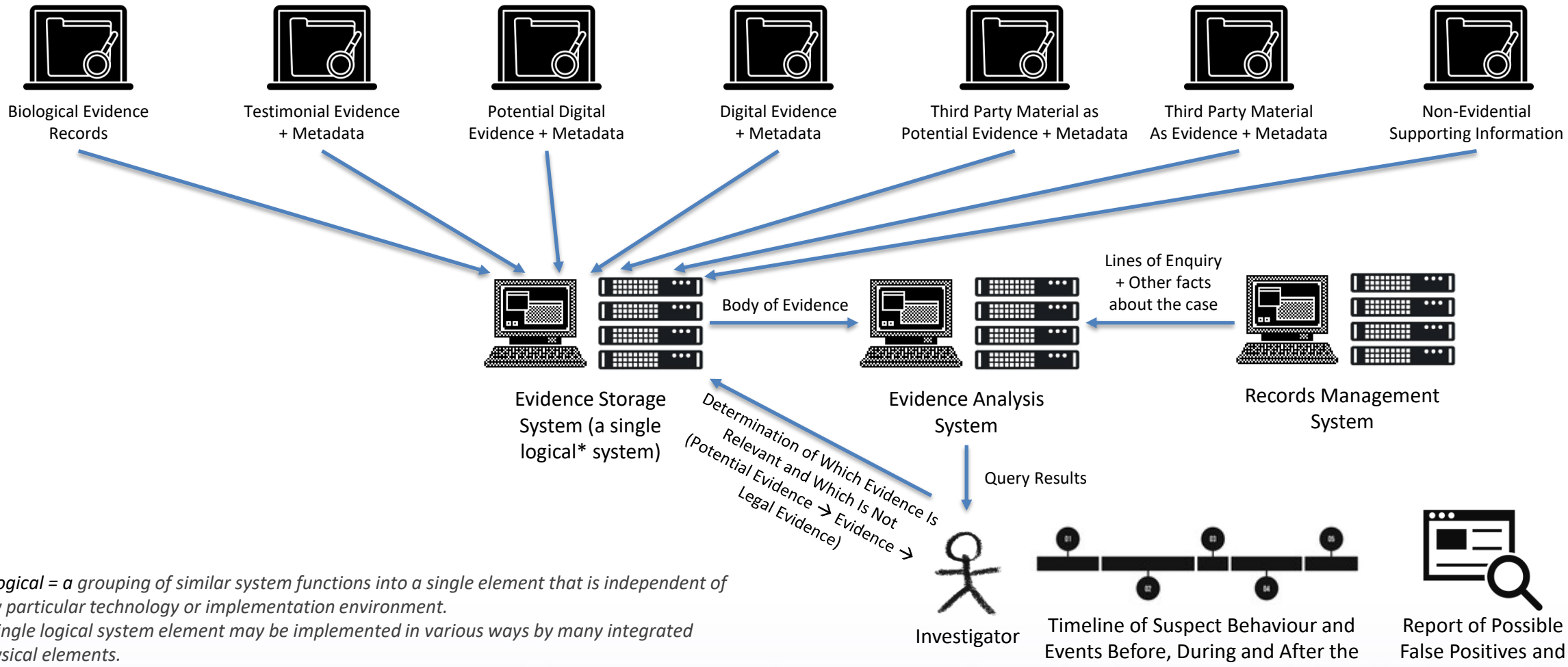


Characterisation of current system architecture

- Silos of evidence by evidence type – difficult to analyse computationally as a body of evidence
- Painstaking sifting and trawling of evidence
- Excel, Excel and more Excel
- Reliance on investigators' hunches, intuition and attention to detail, leading to inconsistent levels of service to victims

- N.B. Because each of England and Wales' 43 police forces are operationally independent, have different systems with different degrees of interoperability, and have each developed their information systems organically over many years, the characterisation of the current system architecture may be inaccurate for many forces. There is no single "As-Is" architecture – the approximation of the current state on the previous slide is the Digital Evidence Project's current understanding and the best representation available.

Characterisation of desired target System Architecture



** Logical = a grouping of similar system functions into a single element that is independent of any particular technology or implementation environment.*
A single logical system element may be implemented in various ways by many integrated physical elements.
In this case the Evidence Storage System would combine discrete items of evidence as a body of evidence for the case. A body of evidence that is queryable, i.e. analysable, as a single logical entity.

Characterisation of desired target system architecture

- A place for everything and everything in its place: accurate metadata and accessibility to support analysis of the body of evidence as a whole
- Analysis of all items of evidence of all types of evidence (testimonial, biological, digital) and related metadata in-the-round at the touch of a button
- A.I. models to identify potentially incriminating and/or substantiating behaviour; grooming, coercion, manipulation, abuse
- Items of evidence associated with lines of enquiry and linked to events to corroborate (or otherwise) victim, witness and suspect accounts of what happened: potential digital evidence becomes digital evidence which is then made available for case file generation as legal digital evidence
- Auto-generation of timeline of events before, during and after the incident, underpinned by evidence, i.e. the story of the incident(s)

Survey questions

- Are we missing any elements in our definition of the problem, or any opportunities? (We don't always have all the answers)
- Do you have any products already in use for evidence analysis and review that we can evaluate?
- Have you got anything ready, imminent or in the pipeline that could meet the analysis and review requirement?
- Is there another organisation you have worked with who you could team up with to deliver a comprehensive solution that meets the needs and expectations of policing with respect to RASSO investigations?
- How can we help develop your tools to meet the needs and expectations of policing?