Computer Law & Security Review 62 (2026) 106348

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Reliability of electronic evidence diagrams – Including a case study of a complex NHS criminal case

Harold Thimbleby *,[1]

Swansea University, Fabian Way, Crymlyn Burrows, SWANSEA, SA1 8EN, Wales, UK

ARTICLE INFO

Dataset link: https://www.harold.thimbleby.net/reeds

Keywords:
Analysing evidence
Computer evidence
Reliability of evidence
Computer support for courts

ABSTRACT

Reliability of Electronic Evidence Diagrams, REEDs, are introduced as a powerful tool to help analyse, communicate, and improve the quality and understanding of computer evidence used in courts. Without REEDs or something similar, defendants and indeed prosecutors have little chance of reaching an adequate understanding of complex dependencies and chains of evidence that are built with (often poorly managed, poorly audited, and poorly documented) computer systems dependent on distributed systems and many vendors. REEDs can also help more rigorously manage IT systems prior to (or to avoid) possible legal action.

REEDs are supported by a prototype innovative tool, making them easy to work with as well as facilitating further research. The tool's source code is available. The tool, which integrates graph theory, visualisation and hypermedia narrative evidence, is a unique feature of REEDs. The underlying textual notation used is light-weight and straight forward to use. REED definitions can be emailed for collaborative work, and the tool's automatic generation of diagrams eliminates the need for artistic skills in visualisation.

Helping improve the analysis and handling of complex computer evidence cases is an intervention of international significance. The REED contribution coincides with the UK Post Office Horizon Scandal (caused by concealed misuse of computer evidence), and coincides with the UK Ministry of Justice reviewing the law and procedures applicable to computer evidence.

The paper includes an in-depth case study of a complex NHS criminal case.

1. Introduction to Reliability of Electronic Evidence Diagrams

This paper introduces *Reliability of Electronic Evidence Diagrams* (abbreviated REEDs) as a tool to help support understanding, critiquing, and refining computer evidence. REEDs are an effective visually-based approach currently based on a simple textual specification language. Complex technical evidence presented visually is a much easier to follow, but REEDs also cross-reference and link the diagrams to conventional narrative evidence, which the REED tool converts to interactive web documents.

1.1. Common problems with computer evidence

Fig. 1 (based on the case study, Section 3) is a characteristic illustration of the common, idealised view that makes it look like the IT is a coherent, simple system. (This view is consistent with the naïve UK Common Law Presumption that computer evidence is reliable [1–3].) In reality, though, any IT system has hidden complexity and numerous factors that undermine its reliability. Factors include: cyberattack, operator error, bugs, networks, cloud system problems, hardware faults, faulty maintenance, incorrect configuration, bad data, and more. In hospital environments, which have numerous computer systems from multiple vendors, there are additional factors such as lack of interoperability, middleware (and multiple versions of middleware), multiple standards partially implemented, poor user training, running obsolete code, code written by unqualified programmers (e.g., poorly programmed Excel spreadsheets), incomplete data because of legacy reliance on paper records, and more. In short, hospital IT systems are very unlikely to be reliable, and possibly unable to provide reliable evidence adequate for use in litigation. Furthermore, few people will understand the IT system and the (un)reliability of its evidence.

Without support to better interpret and challenge computer evidence injustices are likely to follow. Hence this paper's proposal of REEDs to help document, visualise, and think clearly about how IT systems process and construct evidence. REEDs help understand how electronic evidence is formed, routinely processed, and — critically — how evidence may be accidentally or intentionally lost or compromised. Using REEDs encourages disclosing detailed information about

* Correspondence to: 62, Cyncoed Road CARDIFF CF23 5SH, UK.
E-mail address: harold@thimbleby.net.
[1] Emeritus Professor.

https://doi.org/10.1016/j.clsr.2026.106348

Available online 27 June 2026

electronic evidence, and for parties to reach consensus over relevant details. Indeed, if an adequate REED (or equivalent) is not disclosed, the Presumption arguably should be that the operators or owners of the computer system do not know enough about the system and its management — implying that any evidence generated by it is unreliable and should be inadmissible.

The classic review of computer evidence is [4].

1.2. Important features of REEDs

- REEDs help overcome the "inequality of arms" whereby one party (usually the defence) does not have adequate access to or understanding of the computer systems and data processing such that they are not in a position to ask critical questions.
- Although REEDs can be printed as conventional paper documents, on computers, REEDs are fully interactive like well-linked web sites, so clicking on part of the diagram or narrative moves around and navigates the REED document.
- REEDs are designed to be easy to extend as new evidence is considered.
- REEDs enable constructive contributions even when fully informed IT expertise may not be readily available.
- REEDs are effective in pre-proceeding discussions and for courts actively managing cases [5,6].
- Providing REEDs to a court is not burdensome; it follows that being unable or unwilling to provide REEDs (or similar) might be taken to imply that the computer systems and evidence have not been managed adequately, and therefore that evidence is more prejudicial than probative [7].
- REEDs can be very helpful in managing operational computers, and hence for directly supporting clear disclosure on their management and structure.
- A prototype tool for creating and managing REEDs has been developed:
  - The tool was used to draw all REED and other diagrams in the present paper, except for the three historical drawings in Figs. 1, 3 & 4.
  - While the REED tool can generate REEDs in a variety of formats, the most convenient is an HTML web document, which allows users to read and review the evidence by navigating around the chains of evidence easily and intuitively using normal web links. The HTML web document includes an index summarising ideas in the evidence so it is easy to write emails or other web documents that link to specific points of evidence.[2]
  - The tool provides numerous checks that REEDs are complete and consistent, which is particularly useful when REEDs are shared between many people who may make independent edits, potentially leading to unintentional errors and misunderstandings the tool can pick up. The sophistication of the checks provided appears to be unique.
  - The prototype tool makes drawing, checking and managing REEDs very easy. Unlike other drawing tools, the automatic layout of drawings means artistic skills are not required to obtain clear diagrams — and no extra work is required when REEDs are modified (which in conventional approaches would require redrawing diagrams).
  - The tool provides many powerful built-in features to help manage and check evidence, but it also provides open-ended features such as key words and properties (see Section 1.8 and B.6) which can be defined and used in any way as most appropriate for a case.

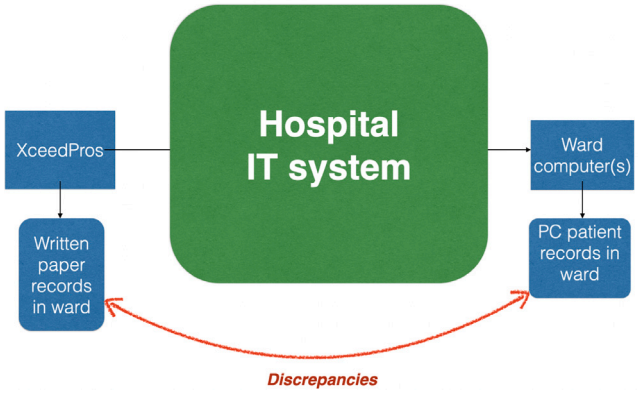

Fig. 1. An original diagram distributed in court. Everybody agreed on this outline of the case, and most thought that the defence case was hopeless because of the (apparently) substantial computer evidence.

The diagram above indicates how nurses use XceedPro glucometers to obtain blood glucose readings from patients. The nurses then record on paper what they have done (as shown on the left). In addition, the XceedPros copy their blood test results to ward computers, but the computer evidence (on the right) showed no blood glucose readings had been taken on multiple occasions.

It was alleged, the nurses fabricated their handwritten notes to show they were caring for patients when in fact they were neglecting them.

The body of this paper explains and illustrates the use of REEDs themselves, regardless of how they are created, whereas this paper's online appendices provide details of the tool and details of how it is used.

1.3. How can REEDs be used?

Preliminary REEDs will typically be drawn up by the parties to litigation in the normal course of their work or by expert witnesses, and then discussed to collaboratively fill in details to create a shared REED, which can be disclosed to all parties. Any remaining areas of uncertainty should lead to further investigations or calling of witnesses. Complex proceedings may require several REEDs, and may require resolution of any inconsistencies between various REEDs.

In some cases involving computer evidence, the prosecution will assume the computer evidence is correct (e.g., in the UK following the Common Law Presumption [1,2,4]), but the defendant team needs to find out *how* the computer systems or their management may have failed. Courts do not like what can turn into 'fishing expeditions' yet IT systems are exceedingly complex, and getting to the root issues in a case is likely to require fishing of some sort.

The REED tool itself makes REEDs from textual descriptions written in normal text documents, and creates diagrams and linked evidence narrative, optionally as interactive web sites. The tool ensures it is easy to perform updates without making a mess of the diagrams or their cross-referencing to the evidence narratives. For instance, the tool numbers each part of a diagram for easy reference, and it automatically keeps the numbers consistent with the relevant sections in the written narratives. Hence as the experts discuss and adjust their REEDs, the tool takes away the drudgery, and also checks for errors like overlooking providing narrative for any part of a diagram. Being based on textual documents, REEDs are easy to email and edit, and do not require any drawing skills. The tool itself is described in some detail in Appendix B,[3] but in the body of this paper I describe *how* it can be used and

[2] Of course, assuming that the HTML web document is on a shared filesystem or is on an accessible web server.

[3] Appendices are available at https://harold.thimbleby.net/reeds.

illustrate how it could have been used to help improve justice in case study involving computer evidence.

REEDs can also be used in the daily management and running of computer systems. If an organisation has an IT audit REEDs can help support this process.

1.4. An evidence map is worth a thousand words

Evidence about computer systems and their data can be very technical and overwhelming, and it may be effectively impossible to see if details are missing or over-simplified. Details are often omitted because it is easier to omit them, there may be accidental or even deliberate inaccuracies, and, anyway, often nobody notices. Indeed, the Post Office Horizon scandal happened because defendants over a long period of time were unable to get at the truth [8].

A common phrase is "a picture is worth a thousand words" — but we do not often think about what that phrase really means.

Take a road map as an example: the map is a picture of all routes from anywhere to anywhere, plus lots of details — from the locations of post offices to national monuments, contours and tidal ranges, gridlines and more. If a map was solely a written document, it would become overwhelming, but when it is a pictorial map, we can pick out any route we need to follow to get to our destination without being overwhelmed with irrelevant detail. Because a map is a picture, we can see details that are relevant to our journey without having to sift through details in other parts of the map. A pictorial map is literally easy to navigate.

REEDs provide a map for evidence, and are particularly effective for complex evidence, such as that originating in connection with computer systems. Although a few symbols are used in REEDs, the key contribution of REEDs is the thorough cross-referencing to sections of textual narrative (possibly with illustrations). Someone reading a REED can go from a symbol on the map of the REED to one or more paragraphs of text explaining it, and from any paragraphs back to the points on the REED map connecting them to the evidence pathways, which are arrow routes on the diagram.

Except in the very simplest of cases, in conventional textual and verbal evidence *some or all* evidential paths will be invisibly missing or over-simplified. REEDs fix this problem because, like a geographical map, a REED diagram is a map showing all possible evidential pathways of interest cross-referenced to detailed narratives, something conventional written evidence cannot make explicit because it would be overwhelming to properly document all possible evidential pathways.

1.5. Evidence coherence

Let us define *evidence coherence* as the quantity of consistent evidence that is relevant, accurate, and makes sense to the mind of the court. The court explores evidence and aims to increase coherence using cross examination and the investigations of expert witnesses, but the evidence also has to have coherence with the underlying facts of the case, yet at the same time the court must not be overwhelmed by trivial, distracting, over-technical or over-simplified 'facts'.

Without further belabouring the definition, suffice to say that increasing coherence is valuable [9], but six factors lower coherence particularly in cases where electronic evidence is relevant:

- Witnesses and the court not understanding complex computer systems and complex evidence from them.
- Computer errors, including cyberattacks and lost or corrupted evidence.
- Inadequate data management and forensic procedures that allow computer evidence to be contaminated, mixed up, or unknowingly corrupted.
- The Common Law Presumption that computer evidence is reliable and therefore need not be scrutinised [1,2].[4]
- There is a tendency to think computers (phones, internet sites, social media, spreadsheets, etc.) are trivial — after all, we are all strongly opinionated on different brands, children can program them, they can be bought over the counter in shops, and you do not need to be an expert to use one. Yet the reality is that computer systems are the most complex systems ever built, and they go wrong in complex ways that are hard to understand and often result in litigation.
- The prosecution will naturally take advantage of any or all of these problems.

A key way to increase coherence is to compare and contrast alternative *views* or characterisations of the evidence. Conventionally, other witnesses will be called, and the various witness statements carefully compared for omissions, corroborations, inconsistencies, or confusions — whether internal inconsistencies or inconsistencies with other statements. The more independent views, the more coherence can be increased by exploring the complementarity of the views. A new view to add, then, is to use a REED.

What a REED does is expand the number of complementary views of conventional narrative evidence, and provides various checks for internal consistency. Primarily a REED does this by:

- Providing a clear diagram of **justified** points of evidence and how they **interrelate**.
- **Annotating** the diagram with highlighting, key phrases, and narrative details.
- Ensuring and confirming everything on the diagram has **corresponding narrative** evidence.
- Ensuring everything in the diagram (and hence in the narrative) is **connected**.
- Allowing the narrative to use **cross-referencing** for clarity, and confirming the cross-referencing is **consistent** with the diagram.
- Providing tables of **tables of contents**, **indexes**, and (if viewed in a web browser) **highly interactive** ways to navigate and explore the evidence.
- Helping write well-constructed, comprehensible reports — for example with automatically numbered sections cross-referenced to the main REED diagrams, along with automatically provided cross-referencing to aid reading and following chains of arguments.
- Making it **very easy** to review, edit and **refine** the evidence diagram and narrative.

Each REED view, as emphasised above, helps increase coherence. For instance, one way REEDs increase coherence is that the narrative-writer can use cross-referencing freely (as in this paper one might cross-reference to another section, such as: "see Section 3.6 for an example of cross-referencing from this paper to the case study REED") *and* the REED tool automatically checks that the cross-referencing links in the narrative are consistent with the chains of evidence represented in the REED diagram.

[4] The case study in this paper, like the Post Office Horizon scandal, is an example of unfortunate consequences of the UK Common Law Presumption; another example is a 2017 case where I was an expert witness. The computer evidence apparently supported the allegation that a nurse had diverted (stolen) drugs. Although many pages of narrative evidence *named* the defendant, I noticed the computer evidence only showed that the defendant's ID had been used to access the drugs. ID is not necessarily the same as the person. It turned out that there were many staff ID cards issued with the same ID, some of which were likely to have been stolen. Hence, the computer evidence was reliable in the sense of giving evidence on an ID, but it was not reliable in terms of prosecuting a *person* who happened to have that ID.

1.6. Improving the reliability of expert evidence

Lord Justice Aikens has noted the increasing technicality of expert evidence, and the length of time needed to present it to the jury and the difficulty for a jury being able to cope with some expert evidence or being able to assess it rationally [10]. Lord Justice Leveson expressed a similar concern [10]:

> "It is, in my opinion, perfectly clear that expert evidence of doubtful reliability may be admitted too freely with insufficient explanation of the basis for reaching specific conclusions, be challenged too weakly by the opposing advocate and be accepted too readily by the judge or jury at the end of the trial. [...] reform is undoubtedly required."

Neither of the Lord Justices noticed that the problem is not just that the evidence and its unreliability and complexity are at issue, but that the generally limited computer competence of the witnesses may undermine evidence making the evidence unreliable through misunderstandings and/or accidental simplification. Lawyers are likely to be unable to properly assess the computer expertise of (so-called) computer experts themselves; it is not just a problem of facts, opinions, or context for a case but of the knowledge and understanding of the witnesses supposedly explaining those technical facts to the court.

The Common Law Presumption that computer evidence is reliable [1,2] further creates a culture where it is harder to establish or even admit that expert evidence or any interpretation of electronic evidence may itself be unreliable — as occurred, for instance, in the Post Office Horizon cases. The Common Law Presumption exacerbates the generally mistaken esteem in which computer "experts" are held.

One argument is that the law itself should be changed to improve standards [11,12], and thus enable courts to engage properly competent experts or reject evidence from those who are not digitally competent to a forensic standard. Another, complementary argument, is the way courts handle computer evidence should be improved — regardless of anyone's expertise. This is the approach explored in the present paper.

In this context, REEDs help assure reliable and intelligible expert evidence because:

- Diagrammatic evidence is easier for non-experts to interpret, follow, and to cross examine.
- The enforced consistency between the diagram and the narrative increases the coherence and reliability of the narrative.
- The diagrams and reliable linkages in the narrative evidence facilitate spotting omissions or other errors in the various chains of narrative assumptions.
- REED features like highlighting and key words help structure and navigate evidence, and help handle related topics together for more reliable examination.
- REEDs allow consistent parts of diagrams (along with their corresponding narrative) either to be extracted or to be excluded, thus allowing the court to focus on a particular concern or, conversely, for the court to exclude a particular concern or concerns from consideration at any particular point.

1.7. Criticisms of diagram-based methods

A powerful criticism of diagram-based approaches is that the diagrams may be merely "PowerPoint Engineering", creating diagrams that deceptively look sophisticated but which conceal engineering oversights. PowerPoint Engineering is an intentionally derogative term introduced by Sir Haddon-Cave in his critical analysis of the total loss of an RAF Nimrod aircraft and all 14 crew and specialists on board in Afghanistan in 2006 [13].[5]

Since REEDs are a flexible concept, misuse of REEDs can indeed lead to the problems of PowerPoint Engineering Haddon-Cave noted, but the emphasis with REEDs is on iterative cooperation where all parties in legal proceedings jointly review, critique and contribute to the developing REEDs and narrative descriptions. Authors and contributors to REEDs will include independent expert witnesses competent in computer science. The social process therefore ensures the REEDs are a constructive, insightful contribution to the proceedings and avoids PowerPoint Engineering — a defence against PowerPoint Engineering is that the REED tool provides numerous checks that a REED diagram is not just a pretty diagram but is properly structured and related to narrative evidence.

A method called Theory of Change (ToC) is widely used across UK government departments and agencies to plan and demonstrate public value [15]. The Government promotes Theory of Change as a way of clarifying ideas for achieving effective change and for reaching consensus on the ideas [15]. Central to the ToC approach, like REEDs, is working cooperatively on the diagrams to agree and make issues explicit, and in particular to help notice critical steps that have not yet been considered. There is an interesting comparison to be made with the Theory of Change and this article's ideas for REEDs. (Section 4.3 uses ToC to present NHS learning points from this article.) Theory of Change, like REEDs, is represented as a diagram of nodes and arrows with connected narratives, with a social process to find and fix problems and to reach consensus. ToC is a comparable approach to REEDs, and its success (and the research behind that success) is an argument supporting the diagrammatic-collaborative process that REEDs also use.

Nobel Prize winner Daniel Kahneman showed our brains process information in two contrasting ways [16], corresponding to fast, automatic, perceptual processing (System 1) and hard, slow, thoughtful processing (System 2). While most diagrams may be arbitrary (and hence raise the PowerPoint Engineering criticism as discussed above) what REEDs do is present evidence in a way that integrates these two modes of information processing. Moreover, the REED approach enables the evidence to be investigated in rigorous ways — Fig. 9, for example, illustrates how a REED diagram can be analysed mathematically *and* diagrammatically, and hence present information in multiple independent ways, thus increasing coherence (defined in Section 1.5).

A REED diagram supports System 1 and the corresponding REED narrative supports System 2, *and* the two representations are tightly connected (by the REED tool) so the twin visual and narrative structures of the REED are complementary and automatically checked as being reliably cross-connected (the cross-connections are themselves visible so can be checked efficiently by System 1). In contrast, in standard approaches, prone to PowerPoint Engineering, evidence presented visually or textually has no necessary or assured connections.

State of the art diagram generators related to REED diagrams, but offering different trade-offs, are summarised in Section 5.5.

1.8. The central REED idea: powerful and easy to use properties

Evidence is not just facts, whether words, sounds or images — in addition, evidence also has *properties*, like who its author or witness is, when it was recorded, what evidence it supports, what evidence it undermines, and so on. Properties are an explicit and central part of the REED approach.

In the REED model, evidence is a narrative which is considered split up into convenient chunks, like paragraphs or diagrams, which REEDs call *nodes*. It is widely recognised that document management can be

[5] The McChrystal Afghanistan PowerPoint slide [14] is a classic example of PowerPoint Engineering.

greatly enhanced by *metadata* [17], but REEDs extend the metadata concept to the internal chunks of narrative evidence, so both nodes and the documents containing them have metadata properties too. Moreover, nodes can be related together using what REEDs calls *arrows*.

In short, REEDs convert conventional narrative evidence into comprehensively linked and easy to use web sites.

Using different language, REEDs convert conventional narrative evidence into hypertext and standard mathematical objects called directed graphs. As such, evidence becomes easy for a human to use and understand (the hypertext perspective), and becomes easy for a computer to manage, analyse, and provide insights about the evidence's implicit structures and potential problems for the user (the graph theory perspective).

Properties in REEDs and their values can be written like this example:

```
author author's-name
```

Since REEDs and their properties are written in ordinary text, easily edited, emailed and shared, and automatically checked, they become convenient tools for clear thinking and better arguments.

A key property of evidence is *influence* (influencing truth, influencing arguments, influencing conclusions, etc.), written in REED style like the following

```
evidence1 influences evidence2
```

The `influences` property is so common — and so useful — it can be written more conveniently with an arrow, usually abbreviated `1 -> 2` or alternatively (but meaning exactly the same) `2 <- 1`, where in this example we have written 1 and 2 to represent arbitrary nodes. The arrow notation allows many shortcuts, for instance `1 -> 2` and `2 -> 3` can be written `1 -> 2 -> 3`.

Using the REED tool, properties and the relations they represent can be visualised diagrammatically. Figs. 3, 4, and 5 in this paper are examples. But much more can be done than just visualising the properties: users can interact with them, they can be analysed, and the REED tool can identify errors and potential errors. In a web document, clicking on part of a REED diagram will take the user to further properties (such as its associated narrative evidence, or other evidence it influences) associated with that part of the diagram.

When a REED is used the evidence and its property relations are converted into an interactive web page; thus in the simple example above, `1 -> 2`, when a user clicks on the evidence 1 they will be taken to the evidence 2. In this (very simplified) example, the REED computer tool will check that 1 and 2 actually have conventional narrative evidence associated with them, and will check more subtle points like if 1 influences 2 and 2 influences another piece of evidence, ... that somehow it does not get back to influence 1 in a big cycle — it is, after all, unlikely that evidence can influence itself, and more likely that some of the cycle is a typo or a misunderstanding of some evidential point. In addition, each node, like 1 or 2 or whatever, requires associated narrative; equivalently, expressed the other way around, each chunk of narrative evidence (like a section or paragraph covering some issue) needs to be associated with a node.

While brief names like 1, 2, 3 are convenient when *writing* REEDs, when *reading* REEDs it is helpful if more meaningful, generally longer, names are used: again, this is done with properties, for instance:

```
CIO is "Chief Information Officer's evidence"
```

This allows (in this case) for `CIO` to be used throughout the REED document for convenience, but displays it to users as the full text, "Chief Information Officer's evidence".

REEDs also allow arbitrarily long narratives as properties; gives an example, which illustrates links, citations, cross-references, key words, coloured flags, and highlighted text embedded in narrative evidence.

REEDs have both pre-defined properties (like `author`, `influences`, `is`) and also allow users to define new properties for their own purposes. `Color` is a simple example of a pre-defined property (with possible values like red, green, fuchsia ...), and colours themselves can also be defined by the user to mean whatever they want. Thus a piece of evidence can be assigned a colour property, such as yellow, and then yellow colouring itself can be defined, as the user finds helpful, for instance to highlight that evidence with the colour property yellow has not been cross-examined. Or pink could be used to highlight evidence written or suspected of being written by AI — and so on without restriction. Of course, users can also use the colour property to automatically extract all evidence of any particular colour for review without the distractions of the entire body of evidence — Fig. 10 illustrates an example of pulling just the yellow nodes out of a much larger REED document.

As an example of the flexibility of properties, they can be used to manage checklists so that parties can raise issues and confirm when relevant issues have been addressed [18]. Note that standard software engineering resources [19] and international standards provide further topics for checklists for electronic evidence.

Mathematicians will recognise REEDs as "Labelled Directed Acyclic Graphs" (discussed further in Appendix A) and programmers will recognise them as "Hypertext". There is a vast literature and body of research on these topics [20–22, etc]. REEDs essentially bring the benefits of these theories and concepts into evidence and hence into courts. Thus standard graph theory concepts like betweenness, component, cycle, degree, path, subgraph, transit node, etc, all have direct legal applications in REEDs — *without the user needing to know any of the mathematical theory*.

An important aspect of these theoretical underpinnings is how REED diagrams support rigorous thinking, specifically *computational thinking* [23] — without the users needing to be aware of the scientific foundations or what the principles are called (just like you can drive a car more safely with ABS regardless of whether you understand how it works). Thus REEDs leverage understanding and thinking about evidence rigorously, by the jury, by legal teams, by witnesses, and perhaps most importantly by expert witnesses.

1.9. The key components of a REED

A REED is a controlled document that has a date, version number, and responsible author(s).

1. A REED may state that the computer system and all other sources and processing of electronic evidence are 'approved devices' (such as speed cameras), and therefore no further details justifying the reliability of the systems will normally be required, beyond statements of truth. At a minimum a REED diagram should be provided to show *how* the device or devices are used and managed, who is responsible for them, and to make explicit the trail of evidence pathways back to reliable sources.
2. In other cases a REED consists of both:

   (a) One or more diagrams showing the major sources and processing of information leading to evidence presented, including relevant sources of information *not* presented in evidence. (Examples are provided in this paper.)

   - All sources, processors, and destinations of evidence, including humans, are called *nodes* in the diagrams. Many processors of information will be computer systems.
   - Nodes are connected by *arrows* showing the flow of evidence data.

(b) A cross-referenced narrative analysis for each node (and optionally each arrow), explaining the purposes and possible limitations of its generating or processing evidence. In addition each node can add arbitrary properties (metadata) to the evidence, for instance to note which systems or laboratories generated evidence data, what questions the evidence raises, and so on.

3. It is expected that a computer tool is used to help prepare REEDs, and such tools will check the consistency, completeness, and integrity of the REEDs. In particular, a tool will assure that relevant narrative analysis has been provided for each node, and that all narratives have associated nodes. In addition, the prototype tool used in this paper produces a digitally signed certificate that it has checked compliance.

2. A note on technical terms used in this paper

It is important to emphasise that users of REEDs do not need to know any mathematical terms or concepts to be able make full use of the tool and to benefit from its features (including its error-checking features). Similarly, readers of this paper may wish to focus on *what* the REED approach achieves rather *how* it works.

Ref. [20] is an excellent introduction to the historical development of graph theory, the main mathematical idea underlying REEDs, from its very earliest — and surprisingly simple — beginnings in 1736. Readers who are more interested in the potential impact and use of REEDs rather than exactly how they work may ignore the technical details.

However, the mathematical thinking behind REEDs assures the ideas reliably scale up to large and complex cases. Researchers interested in the concepts underlying REEDs, or who wish to reproduce the work or develop its novel ideas such as using social network analysis, will appreciate the well-defined, standard concepts used. The prototype REED tool and the case study from this paper are available https://harold.thimbleby.net/reeds

3. The Princess of Wales Hospital case study

This article now presents a REED case study based on the Princess of Wales Hospital 2014 NHS criminal case [24],[6] where 73 nurses were suspended when it was thought that they had neglected patient care, and subsequently five nurses were prosecuted. Three nurses pleaded guilty and received custodial sentences; two pleaded not guilty and went to trial.

The case may be briefly summarised [7,24–26]:

> One of the side-effects of stroke is it can affect diabetes control and can make a sufferer unable to recognise symptoms and control their blood sugar. Accordingly, regular blood glucose monitoring is an essential part of the care of such patients. Nurses working on a specialist stroke ward at the Princess of Wales Hospital, Bridgend, used a handheld blood glucose monitoring device, the XceedPro blood glucometer manufactured by Abbott.
>
> Using the XceedPro, a nurse scans their own staff barcode ID and the patient's barcode, and after a blood reading is then taken with the XceedPro the nurse also records the details on paper.
>
> The measurement data is also stored in the XceedPro until it is docked, and the data is then automatically uploaded to the hospital's database, PrecisionWeb. PrecisionWeb also records other details such as the glucometer's battery level and the temperature of the ward. Ultimately, the data will populate the patient's electronic patient record.
>
> Under normal circumstances, the nurses' written records and the PrecisionWeb database records will be consistent with each other.
>
> There were 130,978 blood glucose readings (together with dates, times, ward numbers, patient and nurse identifiers, etc.) submitted as evidence. It was alleged that the defendants (and the other 68 nurses not prosecuted) had fabricated blood sugar readings to write up in the paper records, so the nurses would have been criminally negligent as the stroke patients had reduced capacity. The prosecution points to the fact that the nurses had written up paper records that did not correspond to anything recorded in XceedPro glucometers nor on the PrecisionWeb database. The situation is illustrated in Figs. 1 and 2.
>
> The expert witnesses pointed out that the evidence was not complete. For instance, PrecisionWeb maintained a 'reject folder' of problematic data (a reject could occur if a nurse ID had been scanned in place of a patient ID, as might happen if the patient's barcode was damaged, just to get the XceedPro to work). In the second week of proceedings, this reject folder was finally produced in court: it contained 18,546 rejected records, but none of the rejected records matched the missing data. The statistical distribution of the reject data very strongly suggested some form of sudden manipulation and (I argued) it was not possible to countenance an explanation consistent with the data being reliable.

In many ways, the case study is a smaller version of the UK Post Office Horizon scandal [1,8,27]; in both, miscarriages of justice were exacerbated by the absurd attitude that computer systems are reliable black boxes, and that evidence generated by computer can be presumed correct.[7]

I was an expert witness in this case and, in court over several days during my cross-examinations, I explained and distributed explanatory diagrams (some are reproduced in Figs. 1, 3 and 4 in this paper) and other details. These diagrams (plus my evidence) were a successful prototype of the more formal REED proposed in this article. Detailed background and more resources, including links to the tool source code, are available at https://harold.thimbleby.net/reeds

Because of the technical analysis presented and clearly communicated by my prototype REED approach, the prosecution called Nick Reece, a PrecisionWeb support Specialist employed by Abbott Diabetes Care.

Mr. Reece had been asked by the hospital to help when the PrecisionWeb database faced problems in 2013. In court, he said he had visited the Princess of Wales hospital on a date that I knew was when data had disappeared from the relevant databases. When asked, he admitted deleting it. The judge concluded that the prosecution evidence was unreliable and was therefore excluded [7]. The prosecution response was to offer no evidence. In consequence, the nurses who had pleaded not guilty were acquitted.

It is noteworthy that the hospital and the prosecution had not previously considered that the explanation of the discrepancies was or might have been that computer data had been deleted rather than the written nurse records had been fabricated by 73 nurses (allegedly colluding to

[6] R v Cahill, R v Pugh, 14 October 2014 at Cardiff Crown Court (T20141094, T20141061). The judge's ruling has been published [7].

[7] The metaphor "black box" implies one cannot see any details inside the box.

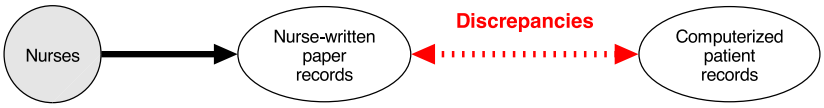

Fig. 2. Nurses' handwritten paper records and the hospital computer records were inconsistent; in particular the computer evidence showed that nurses had not performed some of the tests that they had written up in their handwritten notes. The fact that computer evidence "showing" something may not be reliable evidence had not occurred to the prosecution, and was denied when I raised the possibility, even despite the implausible assumption that 73 nurses had all been negligent and dishonest in their record-keeping in exactly the same way.

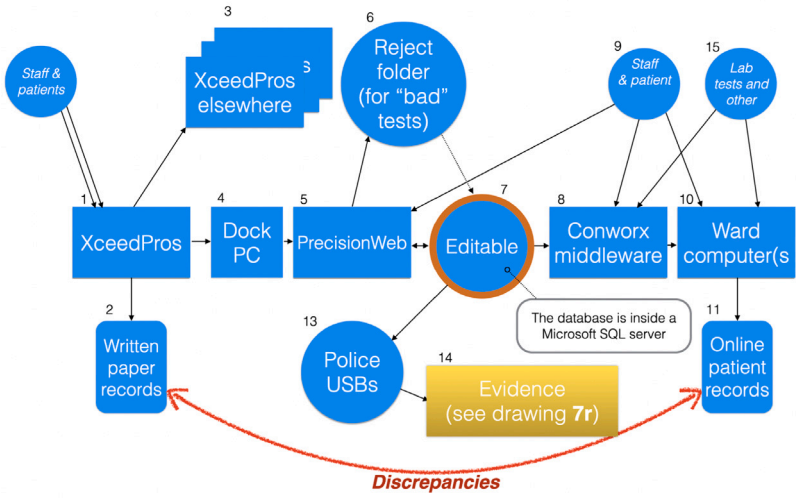

Fig. 3. As shown in this original diagram distributed in court as it became clear that the hospital IT systems were far more complex than the prosecution had portrayed them. For example, the PrecisionWeb database used a data format the main hospital systems did not recognise, so the middleware Conworx was required to change formats. Conworx had hospital technicians managing it, and they would have been able to interfere with its data had they wished.

do so consistently). When I raised such possibilities in pre-proceedings discussion, the prosecution position was that the nurses "were all in it together" — which they asserted without any evidence, and without having explored obvious possibilities such as a bug, hardware failure, a cyberattack, or a computer technician with a grudge. However, prosecuting and terminating the employment of nurses (as happened to many nurses in this case) is cheap and must have appeared as a definitive solution, enabling the hospital to move on. See Section 4.3 for more detail.

3.1. The initial position

Fig. 2, as an alternative perspective of Fig. 1, provides a high-level overview of the Princess of Wales case to make clear the central role of the hospital IT systems. I distributed such diagrams in court to help argue that the hospital IT system was a potentially significant player in the discrepancies that, at that point, had been entirely attributed to the nurses.

Fig. 3 starts to show the real complexity of the hospital system, as cross-examination started to explore the evidence. After a few days, I was able to present Fig. 4 to help explain some of what to me were problems that could undermine the prosecution case (summarised by the judge [7]).

Notice how these hand-drawn diagrams were starting to get complicated, and keeping them up to date, correct, and just neatly drawn was hard — and consequently error-prone.

3.2. Representing the case study with a REED

Based on Fig. 4, we now explore how a clearer and more formal REED, shown in Fig. 5, could be used in the case. This new diagram was drawn with the prototype REED tool, which also ensures its narrative discussion is consistent with the drawing. The complete REED used for the case study can be explored interactively at https://www.harold.thimbleby.net/reeds/pow-reed.html

The REED shown in Fig. 5 is called version 2 because it has already benefitted from information uncovered during the previous weeks of cross examinations. The red warning labels in Fig. 4 are separated from the diagram and put into the narrative evidence, as illustrated in the extracts in Section 3.3 below.

3.3. Example narratives for a REED

A REED has narrative evidence covering all nodes, and optionally for some or all arrows. In the case study, outline narrative evidence was written for this article, but in an actual case the narrative evidence would generally be more substantial.

Two small extracts from the outline narrative illustrate how the police compromised the evidence, moreover in a way that contradicts the Common Law Presumption that computer evidence is reliable.

First, here is an example arrow narrative, extracted automatically for this paper from the full REED narrative with its original typesetting:

> **Arrow E**
> **v2-5.2 Abbott PrecisionWeb database**
> **→ v2-6.3 Police forensic database system**
> **Keyphrases:** CSV; PrecisionWeb database.
>
> The police manually exported a CSV file from the PrecisionWeb database (supposedly) of every record derived from all XceedPros in the hospital over the relevant period of time. This was then copied to a USB stick and taken by car to be copied to the police system, from where multiple CDs were made for copying to the prosecution and defence. **CSV is a non-forensic and very unreliable data format, and the police made no use of checksums or other techniques to assure that the final CDs correctly held the data from PrecisionWeb.**

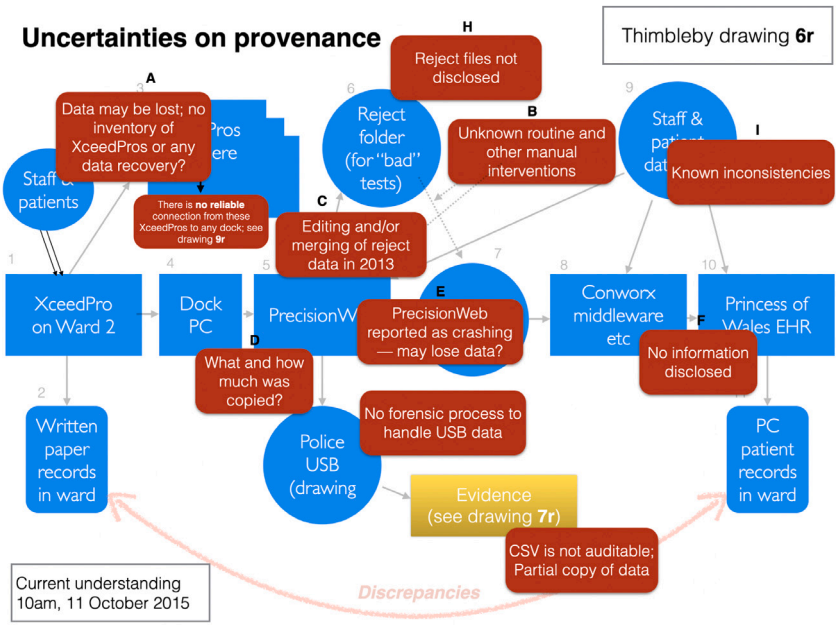

Fig. 4. Another original diagram distributed in court. As the court examined witnesses, it became clear that *the reliability of the police evidence was compromised* — all of the red boxes overlaid on this figure outline serious problems. In particular, the so-called forensic methods used by the police were unreliable.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

In addition, the arrows labelled '**?**' in Fig. 5 indicate evidence flows we *should* know about, but the relevant information was not made available despite requests (it probably does not exist).

Second, here is an example node narrative:

> **Node v2-1.1 Wrong XceedPros seized by police**
> **--- (Group: Police handling of XceedPro evidence)**
> **Keyphrase:** PrecisionWeb database.
>
> The PrecisionWeb data records XceedPro serial numbers, and shows that XceedPros routinely move around the hospital.
>
> **The PrecisionWeb data confirms that the police seized all three XceedPros that happened to be on Ward 2 on the date when they visited it. However, the seizure did not include any XceedPros that had been used by the defendants at the relevant times.**
>
> **In addition to mistakenly seizing the wrong XceedPros, the police sent them to Abbott (node TO v2-2.1 Abbott labs) to be checked for reliability. Abbott unsurprisingly confirmed the XceedPros worked correctly --- it would have been better to chose an independent organization to check the XceedPros.**
>
> **Furthermore, Abbott's evidence says nothing about the reliability of the XceedPros *actually* used by the nurses. Checking the wrong XceedPros is irrelevant to the Prosecution's contention that the nurses fabricated meter readings.**
>
> Reference [24] explains how the police came to seize the wrong XceedPros.
>
> → v2-2.1 Abbott labs
> → v2-3.1 Police summary of wrong XceedPro evidence

3.4. Automatic analysis of a REED

Humans understand evidence by reading it, forming opinions and following links to check their ideas. REEDs enable people to explore evidence and, in particular, routes through the evidence very easily and very thoroughly.

But computer tools can do more, and can contribute insights of a complementary nature to human insights. A REED diagram is a mathematical object called a graph. Graphs have numerous interesting properties: some the REED tool analyses automatically, and some can be analysed by separate tools.

Parts of a graph may be connected to each other but not to other parts of the graph: these parts are called *connected components*. The REEDs shown in Figs. 5 and 7 both have two connected components. In other words, there are essentially two cases at play, some evidence connecting the components has not been disclosed, or some of the evidence may not be relevant. In general, the REED tool lists all connected components, encouraging the evidence authors to consider linking the components.

REED diagrams may become complicated (because the evidence is complicated), and the evidence author may lose track of dependencies. For example, for some evidence $abc \ldots xyz$, we might want z to depend on y, and y to depend on x, and $\ldots$ b to depend on evidence a. But does z really depend all the way back to a? Has one or more of the links been accidentally missed or mistyped in the REED? Consequently, the REED tool allows long chains of evidence to be checked; in this case, the author could write "`check` $a \implies z$" which will check all the links making any path from a to z are present and connected.

Another property of graphs is cycles, chains of evidence that go back on themselves. A cycle is not an error *per se* but may indicate that the authors have not finished working on the REED. Fig. 8 illustrates this point.

Betweenness is one of many powerful social network analysis ideas which can find interesting features of networks. For instance, without knowing anything other than the relevant networks, betweenness can identify critical terrorists in terrorist networks, critical airports in flight networks, or critical power stations in electricity networks. Betweenness has similar utility in evidence networks, as it identifies critical pieces of evidence that many other parts of the evidence rely on. For REEDs, betweenness is a measure of how much a node lies along chains of evidence in the REED narrative network. If the betweenness of a node is high, many chains of evidence depend on it, so high-betweenness nodes are critical to a case.

Fig. 9 is a diagram showing nodes drawn to sizes representing how between they are in the case study: bigger nodes are more between than other nodes. In Fig. 9, it is clear that the PrecisionWeb database evidence has the highest betweenness measure, and an investigator

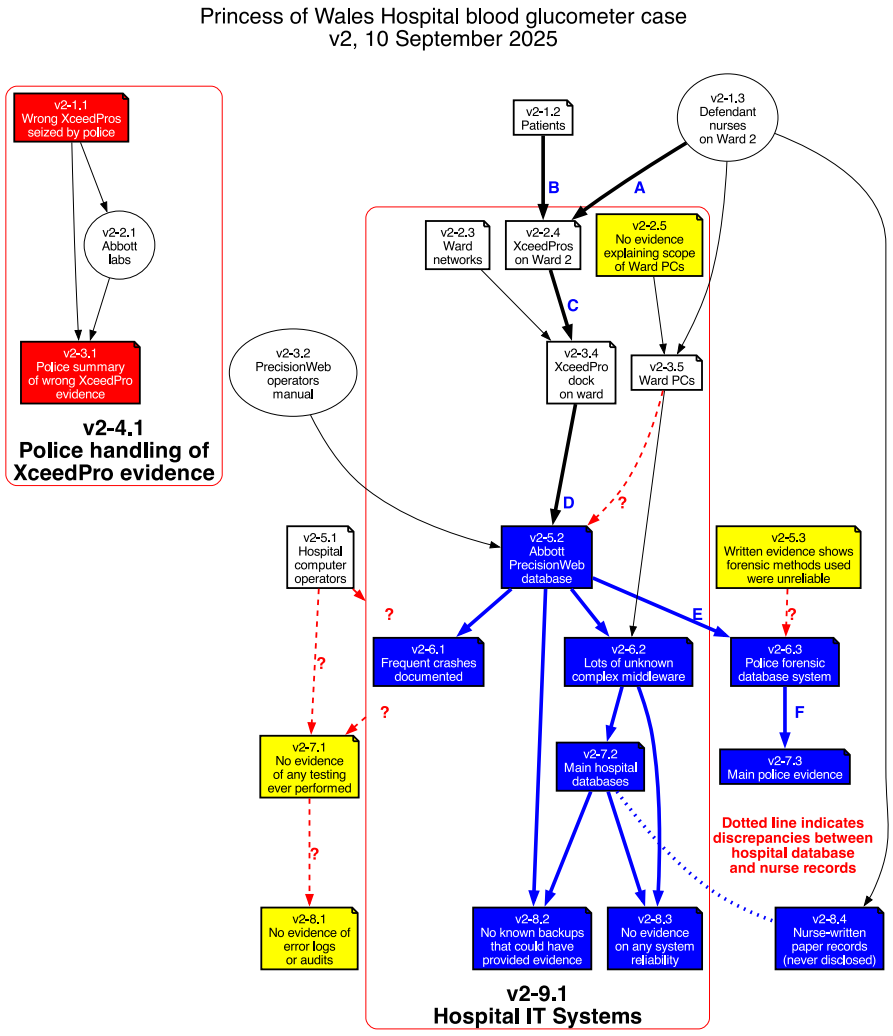

Fig. 5. Redrawing key parts of the original Fig. 4 using the REED tool, also showing some further information that came to light during the early stages of the case. Note that a REED also includes narrative evidence, which is cross-referenced with the nodes and arrows in the diagram — examples of narratives are provided in the article, e.g., in Section 3.3.

Nodes can be highlighted to raise points for attention. In this REED some nodes are highlighted in red to indicate problematic evidence. For a legend for all the colours used here, see Fig. 6. For accessibility reasons or if the printer used cannot show colour, the REED tool can optionally label all nodes with textual colour names.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

blue used 11 times	Version 3 uses blue to highlight the impact of critical new evidence introduced by the Abbott engineer. Only one node was explicitly highlighted blue, but the REED tool is used to automatically cascade the blue highlight to all affected evidence.
red used 2 times	Specific, relevant computer problems as already admitted in evidence. Use of non-forensic tools like Excel (which, for instance, allows rows of data to be deleted *without leaving any record of changing the data*) used to process the evidence. In short, any evidence highlighted in red is unreliable.
white used 6 times	No evidence is available yet. This may or may not be considered a problem after further information is provided.
yellow used 4 times	Evidential problems that have not yet been resolved. Concerns need to be addressed in cross-examination.

Fig. 6. Colour key for the REED shown in Fig. 5. Note that the colour meanings are defined by the REED author, not by the tool.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

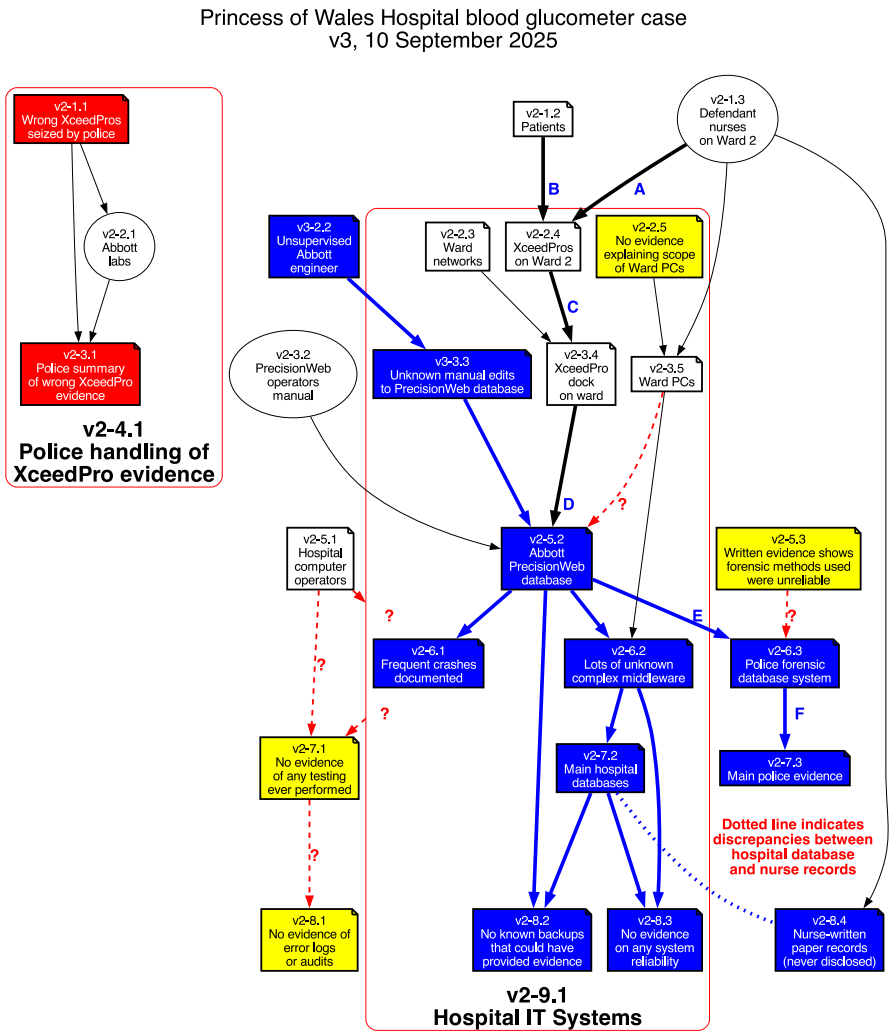

Fig. 7. REED version 3 has introduced a new node (v3-2.2, on the second row of nodes) to represent the evidence of the Abbott engineer's interference. To draw this REED diagram, the REED tool was told to automatically highlight everything affected by the new node in blue, so all the nodes impacted by this new evidence could be appreciated more easily. Clearly, the main police evidence (v2-7.3) has been compromised, and the case's central discrepancy (indicated by the dotted line between v2-7.2 ⋯ v2-8.4) has been discredited.

The colour legend for this figure is provided in Section 3.7. (This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.)

would therefore be recommended to prioritise examining the narrative evidence associated with that node. Indeed, it turned out that the unreliability of the PrecisionWeb database evidence was critical to the case (see Section 3.6).

3.5. Raising and resolving evidential gaps and problems

A REED will typically need updating before and during a case: thinking through a diagram makes it clear that there are more things that need representing, and evidence disclosed or uncovered through cross-examination means more evidence needs representing in the diagram.

The narrative evidence for any REED *must* include a discussion of anything significant that may be missing from the diagram.

Dashed arrows are used in REEDs to show lines of evidence that have not yet been presented to the court. Such lines will be documented in the 'missing' section of the narrative.

Fig. 5 shows node v2-5.1 for hospital computer operators, which begs the questions who are these people, and *who else* has access to the hospital IT systems?

Almost all IT systems have end user licence agreements (EULAs) that allow the manufacturer or developer to deny any warranty for reliability. EULAs are typically very long and tedious; it is suggested that expert witnesses share relevant EULAs and extract any relevant clauses from them for the REED.

For example, the Abbott PrecisionWeb database operator manual specifically says PrecisionWeb cannot be used for clinical purposes, which implies it is not reliable enough for evidential purposes. Its operator's manual [29] specifically says,

> "This product is not for diagnostic use; all patient diagnostics should be based on results reported by the point of care instrument".[8]

PrecisionWeb seems designed primarily to help monitor and maintain XceedPros — for instance to identify low battery conditions that

[8] The PrecisionWeb operator's manual shows that PrecisionWeb is not reliable enough for clinical use; whether it is reliable enough to provide probative evidence for use in court for a particular case is another matter. If PrecisionWeb evidence is used in court (as it was in the case study) there needs to be specific and substantial evidence from Abbott to show whether PrecisionWeb is reliable enough — despite the manufacturers saying it is unreliable in other respects.

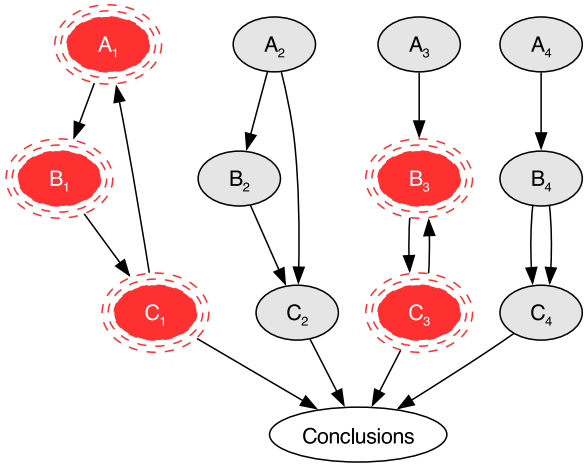

Fig. 8. REEDs generally do not involve circular chains of evidence where evidence ultimately depends entirely or partly on itself (i.e., REEDs are normally acyclic). The diagram above shows how cycles, circular chains of evidential reasoning, are automatically highlighted by the REED tool. In real applications, cycles will likely follow convoluted paths so they will not be obvious without the REED tool pointing them out.

In the illustration above, evidence chains $A_1B_1C_1$ and B_3C_3 form cycles, but is that what was intended? Almost the same chains of evidence could be represented without cycles: perhaps changing the direction of some arrows to make the chains acyclic (as in $A_2B_2C_2$ and B_4C_4) would be more appropriate? The tool cannot make such choices; instead it highlights potential problems, though it can be instructed to ignore specific cycles that are really wanted so they will not be highlighted.

The style used for highlighting (here red nodes with white text and rings of dashed lines) can be changed if required.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

need rectifying. If PrecisionWeb is not reliable enough for clinical use, why is it presumed reliable enough for evidential use?

Fig. 7 makes it clear that there was no evidence available on hospital IT system management or how paper notes were managed, and what (if any) precautions (e.g., to detect and recover from cyberattack or hardware failure) there were in place. I only noticed this as a problem to raise explicitly when I drew Fig. 7, which is the point of using a REED diagram — and then the REED tool automatically required the point to be documented.

3.6. Updating a REED with new evidence

Nick Reece, a PrecisionWeb Support Specialist employed by Abbott Diabetes Care, was called by the prosecution to give evidence. It transpired that the Abbott engineer had unsupervised access to the hospital PrecisionWeb database. The engineer revealed how his 'tidying up' of the database had destroyed the computer evidence that would have confirmed the professional behaviour of the nurses.

The engineer's evidence introduced facts that would have been used to update the REED to a new version, as shown in Fig. 7. With a new node v3-2.2 added, the tool automatically requires additional new narrative text to explain it. Hence the following text was added to the narrative:

> **Node v3-2.2 Unsupervised Abbott engineer**
> **Keyphrases:** Corruption of evidence; PrecisionWeb database.
>
> **Mr. Nick Reece, a PrecisionWeb support Specialist employed by Abbott Diabetes Care, had been asked by the hospital to help when the Princess of Wales PrecisionWeb database faced problems in 2013. Mr. Reece then worked unsupervised on the PrecisionWeb database, apparently taking no notes and certainly not following any forensic process.**
>
> Reece gave evidence that he had failed to take notes on exactly what he did when editing, deleting, and modifying data in the PrecisionWeb database. He admitted he had deleted critical data, which would have created the impression that nurses had been negligent not performing blood glucose tests.
>
> **This deletion of computer evidence explains the discrepancy in patient records that the prosecution claims had been wholly and entirely caused by the nurses' criminal negligence.**
>
> → v3-3.3 Unknown manual edits to PrecisionWeb database

Like other node narratives, the narrative example above has an arrow → showing the evidence node (or nodes when more than one) this evidence may affect, exactly following the connections shown in Fig. 7. The REED tool can also generate HTML narratives, and then the arrow links (both forwards and backwards) become dynamic hyperlinks, so a reader can easily navigate around the structured narrative by clicking on the links.

Although illustrated in this article as Fig. 7 to show how it might have been drawn to support further cross-examination, no new version of the REED was actually needed in court as the prosecution now conceded they consequently had no case. The case was dismissed.

3.7. Using highlighting

Highlighting is used in REEDs as an easy and clear way of flagging nodes and arrows of particular interest.

REEDs do not impose any fixed interpretation for colours, but allow colours to be defined to suit the case.[9] Colours can be used to highlight points of evidence where the experts disagree, and perhaps which should be addressed in cross examination. The REED tool automatically adds highlighting details (as specified by the REED author) to the narrative, as illustrated in Fig. 6. Normally, highlighting affects only specific nodes or arrows, but the tool has a useful feature to 'cascade' highlighting across the diagram. In the case study, the REED authors only needed to explicitly highlight the one new piece of problematic evidence (the unsupervised Abbott engineer and his actions), and the REED tool then automatically propagated the highlighting throughout the diagram (see Fig. 7).

It is notable that node v2-8.4 has now been automatically highlighted because of highlighting the engineer's evidence. Potentially, the nurse-written paper records, which were selected by the Prosecution, are no longer the right records.

3.8. Unresolvable disagreements

It is possible that parties do not agree on the interpretation of some evidence. REEDs therefore allow the narrative evidence to present conflicting statements.

When conflicting notes are made for any node or arrow, the REED tool supports duplicate notes but requires different authors for the notes. The notes are then highlighted, with details of authorship etc, and the diagram has markers drawn on the nodes or arrows to highlight the existence of conflicts. In addition, if parties disagree on the status of a node, they can agree to highlight it with a colour designated to indicate the disagreement.

[9] The REED tool has an option to add the highlight colour as an explicit textual explanation on each highlighted node for accessibility reasons or in case printers do not support colour.

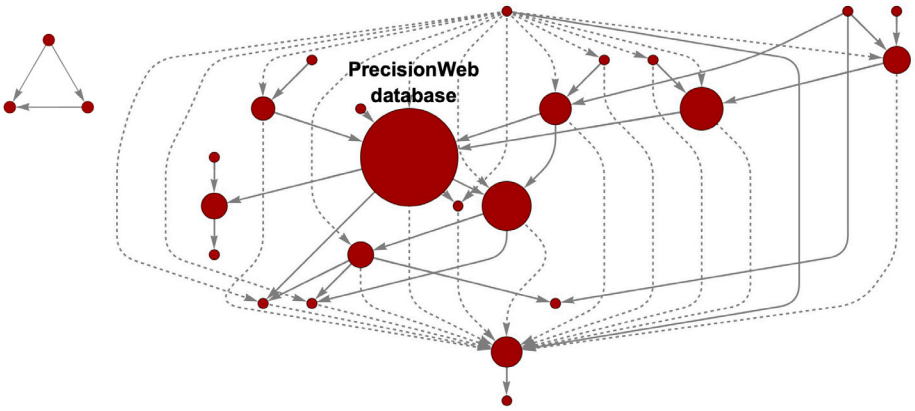

Fig. 9. The REED data from Fig. 7, but shown using a REED tool feature to visualise the evidence relations with the diameter of nodes indicating how many evidential paths each one lies on (hence visualising their "betweenness"), drawn with distracting visual information removed. In other words, the larger the node is drawn, the more the rest of the narrative depends on it. As can be seen, the node with the highest betweenness score for the case study is the PrecisionWeb database evidence itself, which implies the case depends heavily on the reliability of the evidence derived from PrecisionWeb, as well as on its management and the forensic procedures to assure the database itself was reliable.

It is important to note that this visual diagram presents this information in a way that is clear to understand, but which would otherwise be very hard to infer from normal narrative evidence. In fact, PrecisionWeb became *the* central part of the case (see particularly Fig. 7 and Section 3.6).

The diagram above was obtained using Mathematica's standard social network analysis features [28]. The REED tool can export a REED in Mathematica, hence opening up the vast world of mathematical analysis, including many insightful measures like betweenness, centrality, closeness, Page Rank, and more [22].

Some edges may link to groups (e.g., the Hospital IT Systems group in Fig. 7) and therefore implicitly link to all nodes inside those groups. To calculate betweenness correctly here, such edges were expanded into multiple edges explicitly connected to each node in the group. These multiplied-out edges are shown above as dashed lines.

3.9. Simplifying things if REEDs get too complicated

As can be seen from the case study, REEDs can become quite large, even daunting and unwieldy. There are four main solutions:

1. The team working on a REED usually develops it gradually, and it slowly grows and gets more complicated. The team therefore is not worried about the complexity as they are familiar with it.
2. REEDs have a version property. New narrative evidence, new links and properties — or changes to any part of a REED — can be added in or removed from a new version. The REED tool can then generate complete hyperlinked web pages for specified versions.
3. The REED tool can automatically extract smaller REEDs, just selecting nodes that all have the same highlight colour or colours. Since colours normally have helpful definitions (e.g., red might be defined as "Police evidence issues") this approach is a very easy way to separate out coherent, self-contained, parts of a larger REED. Fig. 10 gives a small example, based on the case study. (The highlight cascade feature, described in Section 3.7 and in more detail in the online appendix B.8, makes this a particularly helpful feature.)
4. Similarly, the REED tool can automatically extract smaller REEDs by selecting nodes with specified key phrases: this, then, collects all evidence on a key topic. For example CSV (comma separated values) is a critical topic in the case study evidence, and the tool makes it easy to collate all the CSV-related evidence.

4. Learning points from the case study

The use of REEDs and the details of the case study raise numerous learning points which are summarised in the following sections:

4.1. On reliability

The worked example in this article shows that an apparently reliable hospital system used successfully for years failed, regardless of how long it had previously appeared to be reliable. In fact, the hospital provided no evidence that their computer systems had ever been reliable — there was no auditing or other record that the hospital had ever tried to establish how reliable their systems were. The hospital, the police, the prosecution team including the prosecution experts just assumed the electronic evidence was reliable at face value.

The naïve argument that because computers, blood glucometers, etc, have seemed reliable in the past, or reliable in lots of other places, never means their evidence is reliable for the *particular* case under consideration.

The same style of misleading argument about computer reliability was also made repeatedly in the Post Office Horizon scandal [8,27]: the computer system Horizon worked well for millions of transactions up and down the country so the prosecution would like the court to draw the conclusion that the defendant's Horizon accounts are reliable and therefore prove that the defendant is guilty.

Of course, the very fact of litigation in any case implies *something* has gone wrong, and therefore a blasé dismissal that ignores the specific details of the case is unlikely to be correct.

4.2. For the police: improve digital forensics literacy

The Princess of Wales case study shows how the police's approach to forensic IT investigations was naïve, and in the event counter-productive.

Forensic IT evidence should include features (at a minimum, checksums and digital signatures) so that it can be independently checked for completeness and integrity.

4.3. For the Princess of Wales Hospital

An NHS inquiry followed the court case, *Review of the Blood Glucometry Investigations* [. . .] *establishing lessons learned* [25], and then various committee meetings. Naïvely, the hospital determined that as they had upgraded their wired networks to wifi the problems must have been fixed; moreover the Clinical Director claimed there was nothing for the

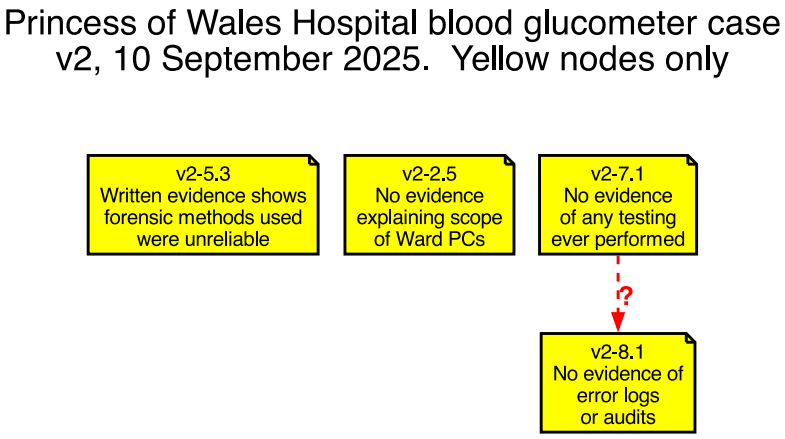

Fig. 10. This diagram was automatically extracted from the REED shown in Fig. 5 by picking out all nodes highlighted in yellow. The corresponding narrative evidence for these selected nodes is also extracted (but to save space has not been shown here). Together the diagram and the corresponding narrative evidence form a concise and focused document — for this REED diagram the meaning of yellow nodes was defined to mean "Problems that have not yet been resolved. Concerns need to be addressed in cross-examination". Other highlight colours for this REED diagram and their definitions are given in Fig. 6.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

hospital itself to worry about because three nurses had pleaded guilty and been convicted.

The Princess of Wales hospital has been widely reported as saying [30]:

> "We can give assurances that regular checks since [the court case] have revealed no further problems.
>
> Issues around the care of patients in the Princess of Wales Hospital, including the blood glucometry test issues, led to the commissioning of the 'Trusted to Care' Andrews Report.[10]
>
> The follow-up review was published last month and gave re-assurances that the care of frail older people is now much better.
>
> We remain determined to do more, to continually improve, and continue to have a commitment to dealing with issues as they arise in an open and transparent way. Like everyone else we have just heard this news about the trial and we will now need to take time to reflect."

On the contrary, the problems exposed by the court case were *not* anything to do with frail older people, but serious problems with the management of computer systems both by the NHS and by Abbott. It is inevitable, then, that the "regular checks" mentioned above as reassurance will continue to miss the underlying problems that have not been acknowledged let alone recognised. The regular checks are unlikely to help if the hospital does not address why it failed to preserve, *and did not realise it was not preserving*, critical clinical evidence it used in a court case. Furthermore, as some nurses pleaded guilty before the case, their cases should be reviewed as the grounds on which they were convicted and struck off are now known to be unreliable.

The expert witness reports to the court contain justified statements like this from a joint report:

> "The database content exhibits serious management issues that have and had not been addressed." [31]

The NHS should have carefully read such expert witness reports, and (given that the case collapsed and therefore did not explore all issues) should have asked the experts for more insights. For instance, the judge pointed out the experts' comments that the hospital had not enabled basic functions the PrecisionWeb database supported to help check the integrity of data [7]. The recommendations of the internal review [25] to involve me on a number of points were never followed up. The hospital chose not to benefit from informed technical insights into their failings.

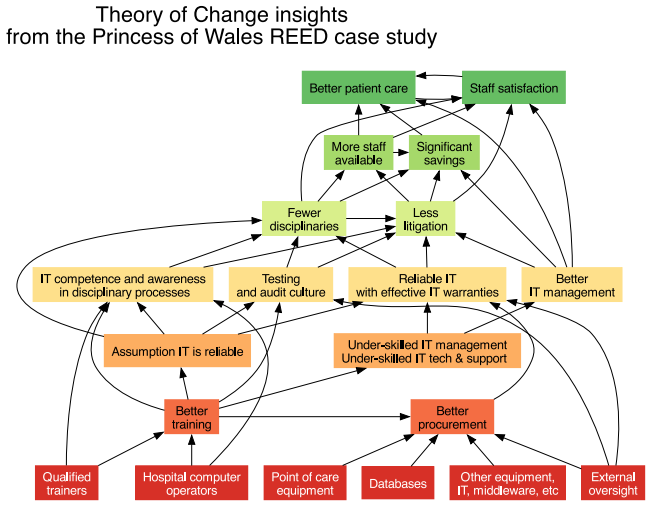

Fig. 11. Visualising insights drawn from this article derived from the REED analyses of relevance healthcare practice, and represented as a concise Theory of Change. Details like resourcing and the high-level planning can be written into the associated narrative, and which the REED tool will link to the diagram.

The diagram above was prepared using the same tool as used to prepare REED Figs. 5 and 7. Although the tool allows the nodes to have cross-referenced explanations, for brevity the narratives are not shown here, despite being generally an important component of a complete Theory of Change.

An interesting application of REEDs is that the tool will automatically require all nodes to have associated narrative, which would help the NHS systematically document their response to the learning opportunities.

(This figure may have been presented in monochrome; for understanding the use of colour in the original figure, the reader is referred to the coloured web version of this article.).

[10] Cited in this article as reference [25].

Written insights, such as the body of this article, are hard to take in, especially in busy non-technical environments like the NHS. Diagrams are much easier to assess. Fig. 11 indicates how a Theory of Change diagram can be used to help *communicate* insights about the hospital case (see also Section 1.7).[11]

4.4. For healthcare and other organisations more generally

This paper raises many insights going beyond the specifics of the case study, raising serious concerns about widespread miscarriages of justice. There are general lessons about the lack of computer expertise available in the NHS (and likely in other organisations), which both led to the situation causing the problems, and led to the NHS mistakenly embarking on disciplinary and litigious actions as a result of its computer problems.

When a court case is supported by computer evidence, it is very likely that known and unknown problems go beyond the defendants and clinical or other specialities involved in the specific case.

Organisations need to vet and supervise everyone with access to IT systems, including visiting computer engineers and police.

A court case stops when it reaches an outcome. The implication is that the organisations should not just read expert witness reports after a case has concluded, but be aware that the reports will have been written before all evidence was available. A case will complete or may be dismissed or collapse for very specific reasons, so wider lessons will be very hard to learn without expert support. Organisations should specifically ask experts to help explain issues that were *not* raised or resolved in court.

For example, the NHS may be aware of the Abbott engineer's corruption of data and that this constituted a problem for the case — although my reading of hospital committee minutes suggests they had no idea. They may not be aware that the lack of supervision of an engineer with unrestricted access to patient and staff data was problematic; the lack of recording what the engineer did was problematic; the reason why an engineer was called in was itself problematic; the reason why the database had deteriorated to such an extent an engineer was requested was problematic; the fact that a badly designed database had been procured in the first place was problematic. (See https://harold.thimbleby.net/reeds and [31] for additional documentation.)

Until the NHS and other healthcare providers recognise IT problems as such and acknowledge that they are symptoms of poor IT skills and management, and are not just specific past historical problems with specific hospital systems the healthcare providers and their suppliers will not be able to avoid more problems and avoid further disruptive and expensive miscarriages of justice in the future.

IT systems should be continually monitored for cybersecurity breaches and other losses (and corruptions) of data: the Princess of Wales case study shows that the hospital would be unable to detect a cyberattack that deleted data [24]

Copies should be made of any evidence taken — in the Princess of Wales case, the evidence taken was in CSV format, which has no protection against accidental or deliberate editing, and there was no way to check the police evidence was the same as the original PrecisionWeb data.

Regular testing should be undertaken to check that IT systems are working as expected, and logs should be treated as controlled documents.

Expert witnesses need access to IT systems, their documentation, test procedures and logs, as well as their operators and managers (the Princess of Wales took the position that a criminal case was underway and no access was permitted).

4.5. For Abbott, manufacturers generally, and regulators

As this paper showed, disciplinaries, suspensions and prosecutions followed from the unfortunate actions of Mr. Reece, the Abbott engineer who deleted data and caused the impression that nurses had been negligent. Arguably, the database and glucometers should have been designed so that loss of data without any record would not have been possible. It appears that Abbott, the manufacturers, performed no investigation into the problems of the design of their systems or into the actions of their engineers. It follows that new devices and systems will not benefit from any learning from the case, and the weaknesses may be perpetuated in future designs.[12] Similarly, the relevant UK regulator, the MHRA (Medicines & Healthcare products Regulatory Agency) showed no interest in the case, despite the fact that the systemic issues the case exposed about hospital devices and computer systems are endemic [26].

5. The future of reeds

5.1. Why current REEDs are simple

REEDs link textual, narrative, evidence with an evidence pathway diagram. As currently implemented, a REED is defined using a very simple text file, as described in Appendix B. The definition file can be written in any order and split up without restriction; it can be edited with any text editor. This makes REEDs very simple to use and easy to learn, as there are no superfluous features to learn or which might have compatibility issues with other software.

On the other hand, most comparable systems provide many features and integrate editing, note-taking, diagramming, networking, and collaboration features — this makes them more powerful, but also makes for steeper learning curves, as well as providing lots of integrated features that have nothing to do with narrative evidence. Often, unlike current REEDs, the underlying data or database is proprietary not easily sharable. In other words, to get more features, these systems tend to lock in their users making it harder to share data and collaborate across and between organisations.

The point of making REEDs so simple is to help focus on how the ideas facilitate understanding complex evidence, investigating and critiquing it. More features could be a distraction.

5.2. Limitations of REEDs and making them easier to use

REEDs can be printed on paper and are easy to use: they present a comprehensive analysis and visualisation of evidence. The prototype tool offers one way to generate and manage REEDs: the prototype tool emphasises the value of being able to email and share purely textual documents that are easy to read and edit. Other trade-offs might be made, for instance emphasising direct manipulation drawing of the REED diagrams — however the prototype tool does all diagram layout automatically and thus relieves users from the often tricky layout problems of making diagrams readable and look neat (which often has to be done repeatedly as users update the evidence narratives and diagrams).

The idea of connecting diagrams to text, as REEDs as described in this paper, is not new. There are many note-taking and productivity tools such as Coda [32], Logseq [33], Notion [34], and Roam [35] that work a bit like REEDs. While these tools provide some of the benefits of REEDs, they focus more on:

[11] It is almost inevitable that a reader of this article will immediately think of ways to improve the Theory of Change shown in Fig. 11 — but that is exactly the point. By negotiating and adopting suggestions, the Theory of Change — or a REED — will improve in value to the parties working with it.

[12] I wrote to Abbott 28 April 2025 inviting comments on this article, and specifically on the statements in Section 4.5, but have not (yet) had any reply. If Abbott has any reviews, I would welcome seeing them (even, if need be, under an NDA).

Flexibility Rather than providing features specifically aimed at one task well (such as supporting evidence), note-taking tools focus on general purpose features that can do anything and therefore are weak on checking.

Ease of use These note-taking tools are integrated with user interfaces for multi-user note-taking. In contrast, REEDs are based on ordinary text files, and allow users to work with any editors.

Markdown These note-taking tools support stripped-down versions of HTML ('markdown') for formatting. In contrast, REEDs can use standard HTML or LaTeX.

Communities Most note-taking tools are supported by large communities of developers, and therefore fixing bugs and adding new features is easier.

Wikis Many note-taking tools are based on wikis [36], including Coda, Notion and Roam (with Logseq supporting wiki features with a plugin).

Specific application areas Section 5.5 briefly reviews tools designed for specific application areas such as presentations and eDiscovery [5] supporting digital forensic investigations.

Easy to use multi-user collaboration and interactive ways of editing documents are useful features the current paper has not addressed. Future work will therefore likely to combine the best from easy to use productivity tools and REEDs.

5.3. Supporting arbitrary extensions to REEDs

REEDs enable simple built-in extensions to help support complex investigations, such as highlighting nodes. The REED approach has no preconceived use of highlighting, and users can use colours to have arbitrary meanings to suit their requirements.

However such flexibility may not be powerful enough for all purposes. The question arises: how can REEDs support *unanticipated* extensions, for instance as might be required in managing evidence from multi-jurisdictional or complex financial fraud investigations?

Nodes and arrows, which can already be coloured for arbitrary purposes and annotated with arbitrary text, can also be annotated with metadata (meta information) for any named properties [17]. For example, metadata can be used to annotate a node or arrow with its country of origin, location of sources of evidence, glossary and other definitions, outstanding queries about the node, names of people to ask for clarification, dates when labs will complete tests, the date when the node was added to the REED, whether the node's accuracy has been checked, previous cases, references (including URLs) … The metadata can be *anything* that might be useful: information about nodes or arrows in addition to the REED's primary use of keeping track and documenting which nodes depend on or are influenced by other nodes (and analysing the consequences of those dependencies).

The current prototype REED tool has no built-in interpretation for metadata properties; instead it can summarise all metadata and extract metadata properties in a CSV file which can be readily processed in general purpose tools like Excel, printed as conventional written evidence, or passed to special purpose tools, including AI as appropriate. The REED tool can also generate XML and Mathematica files [28] with all nodes and metadata for arbitrary processing as required.

Further details are given in the appendix, section B.6.

5.4. REEDs could be treated like car MOT certificates

The UK Road Traffic Act 1956 introduced MOT[13] certificates, which at first only covered brakes, lights, and steering. MOTs were optional until 1961.

MOT certificates are now a legal requirement, and cover many points including tyres, emissions, seat belts, chassis, bodywork, wipers, driver's view of the road, and wiring, etc. Since 2018 drivers can face fines if their cars are not roadworthy regardless of possessing a valid in-date MOT certificate; put in other words, drivers can face fines if they would not be able to obtain a valid MOT given the current state of their car.

In the UK it is illegal to drive a car without a MOT certificate (if it requires one, for instance because it is not a new car of an approved design). If a car is involved in an accident, insurance and courts take the absence of an MOT as contributory negligence and may increase penalties. The absence of an MOT also invalidates insurance, and it very likely reduces compensation (if any is due) to the owner and occupants of cars without a MOT.

Car MOT law inspires an analogy with proceedings depending on computer evidence:

> If a court handling computer evidence is not presented with a competent REED or equivalent to support informed cross examination then the Presumption should be that the computer evidence is incomplete and unjustified — and likely misleading.

Like the history of car MOTs, it is proposed that REEDs should be introduced in a simple form, then increasingly tightened and improved with experience of their use.

Unlike MOTs, which are summary certificates that a car meets the minimal requirements to be roadworthy, REEDs also enable the sources and management of evidence to be critiqued, and help parties achieve a common understanding of technical issues and weaknesses. However, if the MOT analogy is pursued further, REEDs are also like MOT *advisories* in that they raise specific problems and concerns that need addressing. Indeed, an interesting analogy with MOT certificates is that in the same way that drivers can use their MOT advisories to help plan maintaining their vehicle, REEDs can be used routinely by organisations to manage and gain insights into the state of their IT systems.

New cars do not need MOT certificates because they are assumed to be well-designed, well engineered, and road worthy (in a process called homologation, where the design and manufacturing process themselves are certified). Likewise IT developers and vendors might like to provide REEDs (or a variation of REEDs) as evidence their products are reliable and easy to understand and hence help procurement processes. In fact, cars have a separate voluntary system of safety, performance and environmental ratings, which has contributed to a dramatic increase in car safety and reduced environmental impact. These visible voluntary rating systems have also helped consumers become better informed, which in turn has pressurised the market, and led to improvements in manufacturing. A similar approach might be used for computer systems.

Car design and development is a mature, well-regulated industry. In contrast, computer systems are neither mature nor well-regulated, so the MOT analogy has limitations. Outside of safety critical industries (such as nuclear power) there has been very little interest in, and even resistance to, assuring computer systems are dependable. Even for medical devices, the regulation is years behind any effective oversight of the growing complexities of medical computer systems, particularly — but not just — AI [26].

[13] MOT is an abbreviation for Ministry of Transport, now a defunct Government department subsumed into the current Department for Transport.

5.5. State of the art and alternative approaches to REEDs

Further research is called to assess, develop, refine or find better notations and approaches to REEDs. Alternative approaches — along with powerful tools — have been found helpful in other application areas, include:

- There are many easy-to-use drawing tools (including Apple's Keynote and Microsoft's PowerPoint) that can be adopted to help draw REEDs and write the narrative evidence. However, such tools provide no checks and no automatic cross-referencing.
- There are many tools used in eDiscovery (i.e., identifying, collecting, preserving, and analysing digital evidence), some of which have powerful graphical facilities [5]. eDiscovery is concerned primarily with finding and preserving electronic evidence while maintaining a strict chain of custody; in contrast REEDs can help organise and structure any evidence, particularly narrative evidence and points from cross examination.
- Safety assurance diagrams [37], such as Adelard's ASCE (the Assurance and Safety Case Environment) [38]. Safety assurance diagrams are primarily concerned with making rigorous arguments about safety (e.g., for the design of a computer system).
- Theory of Change diagrams [15] (see Sections 1.7 and 4.3).
- Unified modelling language, UML [39].
- Why-Because Analysis, WBA, and Why–Because Graphs, WBG [40].
- Many integrated techniques for rigorously developing software and documentation together, such as DRisQ's System Kapture [41], and the National Security Agency's/Praxis's Tokeneer [42].
- The Semantic Web [43], along with its technologies like RDF (Resource Description Framework), is a now mature general approach to knowledge representation, which has many ideas and tools that could fruitfully cross-fertilise with REEDs.

5.6. Continuous improvement

People using REEDs will no doubt have diverse experiences and ideas, and perhaps spot bugs and design issues that they may have views on improving or extending. When REED authors have any thoughts, they are encouraged to use the REED command `feedback` *`idea`* and then that idea will be sent to Harold Thimbleby. For example:

```
feedback   "Although REEDs can already be exported
           as XML, why not use Office Open XML to make
           it easier to convert to Word documents?"
```

6. Conclusions

This article introduced REEDs, Reliability of Electronic Evidence Diagrams, as a practical way to explore and improve the details and reliability of computer evidence. A REED consists of one or more evidence diagrams and linked narrative evidence. They significantly improve evidence *coherence* (a term defined in Section 1.5): that is, they broaden the ways in which evidence can be created, shared, and critically examined.

REEDs rigorously combine visual and narrative evidence, improving understanding, and reducing the chances of unnoticed errors (since the same information has to be represented in multiple ways). The prototype REED tool provides significant checking to spot errors, and to support writing consistent, high-coherence evidence. REEDs additionally support rigorous, independent checking of evidence using independent widely-available professional tools such as Mathematica. For instance, "betweenness" analysis (directly supported by Mathematica, explained in Fig. 9 and mentioned in Section 1.7) is only one of thousands of independent, rigorous ways to critically analyse REED evidence. In general, using REEDs one would expect anomalies or inconsistencies in evidence to be rapidly uncovered, and as experience with REEDs grows, the best ways of checking evidence with them will spread.

A large NHS criminal case was used as a case study, showing that the REED technique scales up to real complex cases. It appears, more generally, to be of benefit to investigations by facilitating clearer and more reliable use of electronic evidence.

The REED diagrams in this paper were drawn using a prototype tool that drew the diagrams and managed the corresponding narratives using a simple text file format.[14] The tool has three key advantages: it checks for errors (such as missing narrative sections); being entirely textual it is very easy to email and edit and involve others to review diagrams and narratives; and because the diagram itself is drawn automatically, the tool means that no special drawing skills are required to draw clear diagrams.

It is arguable that had REEDs been used routinely by the Princess of Wales Hospital to support more critical operational IT management, then the IT problems leading to the criminal case would have been uncovered and addressed earlier, or the hospital's investigations, even if they could not fix problems, would have understood their problems and thus not progressed to suspensions and prosecutions. Certainly the diagrams used in court (Figs. 1, 3, and 4) would have been much easier to prepare and polish — and ensure complete! A collection of resources and further commentary on the case study is provided in Ref. [31].

Importantly, with the clarity of REEDs, the court case may have been resolved in a way that the clinical staff and leadership in the hospital would have understood their computer management problems so the Princess of Wales Hospital would have subsequently taken appropriate corrective action, which, in the event, it did not. Section 4.3 (above) shows that despite the findings of the court and even its own internal investigation, the hospital still failed to make any use of the technical insights: it did not understand the court's findings, most likely because it did not understand its own computer systems and operations. This paper's support web site https://www.harold.thimbleby.net/reeds provides some public domain committee minutes that support this apparently harsh criticism.

The use of REEDs could be researched to establish how parties can best work using them, and to identify and evaluate possible ways to improve them (see 5.5 for alternative and complementary approaches). Standards could also be developed, as courts could find it helpful to be able to check REEDs are prepared to conform to relevant standards.

Improving the quality of computer evidence and improving the ability to critically examine computer evidence will, in the longer run, help improve the quality of computer systems and computer system management, and hence reduce litigation based on misused and misleading computer evidence.

Funding

This research did not receive any grant from funding agencies in the public, commercial, and not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[14] Figs. 1, 3, and 4 were drawn as freehand diagrams in 2014 using Apple Keynote, a program similar to Microsoft PowerPoint. All other diagrams in this article were drawn by the prototype REED tool.

Acknowledgements

Kirsty Brimelow, Leo Freitas, Peter Ladkin, Stephen Mason, Paul Marshall, Rachel Cahill-O'Callaghan, Prue Thimbleby, and Martyn Thomas.

Online appendices (supplementary data)

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.clsr.2026.106348.

Data availability

For all data and source code, please see https://www.harold.thimbleby.net/reeds.

This web site includes links to the Git repository for the REED source code and various REED files, including the full NHS case study REED used in the paper.

References

[1] Christie J. The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence. Digit Evid Electron Signat Law Rev 2020;17:49–70. http://dx.doi.org/10.14296/deeslr.v17i0.5226.
[2] Ladkin P, Littlewood B, Thimbleby H, Thomas M. The Law Commission presumption concerning the dependability of computer evidence. Digit Evid Electron Signat Law Rev 2020;17:14. http://dx.doi.org/10.14296/deeslr.v17i0.5143.
[3] Mason S. Electronic evidence: A proposal to reform the presumption of reliability and hearsay. Comput Law & Secur Rev 2014;30:80–4. http://dx.doi.org/10.1016/j.clsr.2013.12.005.
[4] Mason S, Seng D, editors. Electronic evidence and electronic signatures. 5th ed.. Institute of Advanced Legal Studies for the SAS, Humanities Digital Library, School of Advanced Study, University of London; 2021, URL https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures.
[5] Lawton D, Stacey R, Dodd G. eDiscovery in digital forensic investigations. Publication 32/14, Centre for Applied Science and Technology (CAST), Home Office; 2014.
[6] Woolf H. final report to the lord chancellor on the civil justice system in England and Wales (access to justice). Stationery Office Books; 1996.
[7] Crowther QC H. CASE RULING: ENGLAND & WALES Case citation: R v Cahill; R v Pugh. Ruling 14 October 2014, Crown Court at Cardiff. Case numbers: T20141094 and T20141061. In: Digital evidence and electronic signature law review. Vol. 14, 2017, p. 67–71. http://dx.doi.org/10.14296/deeslr.v14i0.2541.
[8] Brooks R. Post mortem. Private Eye Productions; 2025.
[9] Smith K, Shaw G. Achieving Best Evidence in Criminal Proceedings. Ministry of Justice; 2011, URL https://assets.publishing.service.gov.uk/media/6492e26c103ca6001303a331/achieving-best-evidence-criminal-proceedings-2023.pdf.
[10] The Law Commission. Expert evidence in criminal proceedings in England and Wales, law com no 325, HC 829. London: The Stationery Office; 2011.
[11] Thimbleby H. A framework to update the Common Law presumption that computer evidence is reliable. In: Parsons M, editor. AI and safety critical systems proceedings of the 34th safety-critical systems symposium, vol. SCSC-208 of **SCSC-200**, safety-critical systems club,. 2026, p. 433–47.
[12] Thimbleby H, Thomas M. The Post Office Horizon Scandal: Ensuring nothing like it ever happens again. In: Parsons M, editor. Developing safer systems, proc 33rd safety-critical systems symposium. SSS'25, 2025, p. 361–76, SCSC-199.
[13] Haddon-Cave C. The nimrod review — an independent review into the broader issues surrounding the loss of the RAF nimrod MR2 aircraft XV230 in Afghanistan in 2006. House of commons, UK government; 2009, URL https://www.gov.uk/government/publications/the-nimrod-review.
[14] Davies R. Everything i know about life i learned from powerPoint. Profile Books; 2021.
[15] Department for Environment Food & Rural Affairs. DEFRA theory of change (ToC) tool. 2021, URL https://randd.defra.gov.uk/ProjectDetails?ProjectId=20910.
[16] Kahneman D. Thinking, fast and slow. Macmillan; 2011.
[17] Pomerantz J. Metadata. The MIT Press Essential Knowledge series, MIT Press; 2015.
[18] Gawande A. The checklist manifesto, How to get things right. 2011, Profile.
[19] Sommerville I. Software engineering. 10th ed.. Pearson Education; 2017.
[20] Biggs NL, Lloyd EK, Wilson RJ. Graph theory 1736–1936. Oxford University Press; 1986.
[21] Gross JL, Yellen J. Graph theory and its applications. 2nd ed.. Chapman & Hall/CRC; 2005.
[22] Kadushin C. Understanding social networks, theories, concepts, and findings. Oxford University Press; 2012.
[23] Curzon P, McOwan P. The power of computational thinking. World Scientific; 2017.
[24] Thimbleby H. Misunderstanding IT, Hospital cybersecurity problems in court. Digit Evid Electron Signat Law Rev 2018;15:11–32. http://dx.doi.org/10.14296/deeslr.v15i0.4891.
[25] Hopkins A. Review of the blood glucometry investigations in Abertawe Bro Morgannwg University Health Board, Establishing lessons learned. 2016, URL https://www.harold.thimbleby.net/glucometry-records/Hopkins-report.pdf.
[26] Thimbleby H. Fix IT: see and solve the problems of digital healthcare. Oxford University Press; 2021.
[27] Wallis N. The great post office scandal: the extraordinary story behind the major ITV drama: the fight to expose a multimillion pound IT disaster which put innocent people in jail. Bath Publishing, Limited; 2021.
[28] Wolfram S. The mathematica book. 5th ed.. Wolfram Media Inc; 2004.
[29] Abbott Diabetes Care Inc. Precisionweb, point of care data management system user's manual QC, Manager 3.0. 2009.
[30] Wright B. Nurses accused of neglecting patients at Princess of Wales cleared as case collapses. In: Wales online. 2015, URL https://www.walesonline.co.uk/news/wales-news/nurses-accused-neglecting-patients-princess-10258426.
[31] Thimbleby H. Archived Princess of Wales glucometer documents and notes. 2024, URL https://www.harold.thimbleby.net/glucometry-records.
[32] Coda. Your all-in-one collaborative workspace. 2025, URL https://coda.io.
[33] Logseq. Connect your notes, increase understanding. 2025, URL https://logseq.com.
[34] Notion. Notion for notes & docs. 2025, URL https://www.notion.com/notes.
[35] Roam. A note-taking tool for networked thought. 2025, URL https://roamresearch.com.
[36] Chatfield TB. The complete guide to wikis how to set up use, and benefit from wikis for teachers, business professionals, families, and friends. Atlantic Publishing Group; 2009.
[37] The Assurance Case Working Group (ACWG). Goal structuring notation community standard, Version 2. 2018, URL https://scsc.uk/r141B:1?t=1.
[38] Adelard. ASCE: The assurance and safety case environment. 2025, URL https://www.adelard.com/asce.
[39] ISO/IEC Technical Committee JTC 1. ISO/iEC 19501:2005 – information technology – open distributed processing – unified modeling language. UML, Geneva, Switzerland: International Organization for Standardization; 2005, URL https://www.iso.org/standard/32620.html.
[40] Ladkin P, Loer K. Analysing aviation accidents using WB-analysis — An application of multimodal reasoning. In: Spring symposion. AAAI Tech Report SS-98-04, Association for the Advancement of Artificial Intelligence; 1998, p. 169–74, URL https://www.aaai.org/Papers/Symposia/Spring/1998/SS-98-04/SS98-04-031.pdf.
[41] D-RisQ. Kapture. 2025, URL https://www.drisq.com/kapture-more-about-information.
[42] Cristiá M, Rossi G. An automatically verified prototype of the Tokeneer ID station specification. 2020, URL https://arxiv.org/abs/2009.00999.
[43] Hitzler P. A review of the Semantic Web field. 64, (2):2021, p. 76–83. http://dx.doi.org/10.1145/3397512,