DEEP:

Extending the digital forensics process model for criminal investigations.

Dr Jan Collie, STEM Computing & Communication

Jan Collie

- Lecturer in Cyber Security,

  The Open University

Richard Overill

- Visiting Senior Research Fellow in Cyber Security,

  King’s College London

Digital Evidence

- Integrity
- Best practice

- Issues:

- Compromised
- Tainted
- Destroyed
- Overwritten

Problems:

- Training

- House of Commons Justice committee on Disclosure of evidence in criminal cases (2018).

> ‘One of the big issues that I see… is that the digital forensics units are quite good at keeping up to date with technology for extracting data and making copies, but they then pass the copies, largely uninterpreted, to police officers, who are not experts and who are not digital forensics people. General policing investigators do not necessarily have the tools to search that information effectively and understand it.’

Forensic Science Regulator, Dr Gillian Tully

> ‘Typically, police with limited digital forensic expertise have the initial responsibility to recognize sources of digital traces and to apply basic preservation and processing methods. They are at high risk of not realizing limitations in the methods and tools that are available to them, leading to mistakes and missed opportunities.’

Casey E. (2019)

Problems:

- Accurate analysis

- House of Lords Select Committee on Science and Technology (2018)

‘The delivery of justice depends on the integrity and accuracy of forensic science evidence and the trust that society has in it.’

- Casey et al. (2018)

the ability to interpret digital evidence accurately is crucial in order to ‘avoid mistakes, missed opportunities, misinterpretations and miscarriages of justice.’

- Collie (2018)

‘Digital forensics is meant to be based on science, not supposition. And in every case, somebody’s freedom is at stake’

Problems:

- Volume & Funding

- House of Lords Select Committee on Science and Technology (2018)

> ‘It is clear, from the evidence that we have heard, that the growth in digital material presents a challenge to police and prosecutors. We believe that police forces are not always adequately equipped or properly trained to handle the type and volume of evidence that they now routinely collect and that this can lead to errors when reviewing and disclosing material and therefore has the potential to lead to miscarriages of justice.’

Problems:

- Confirmation bias

- Shaw and Browne (2013) - potential to misinterpret data by inadequately trained personal

  - Casey (2018).

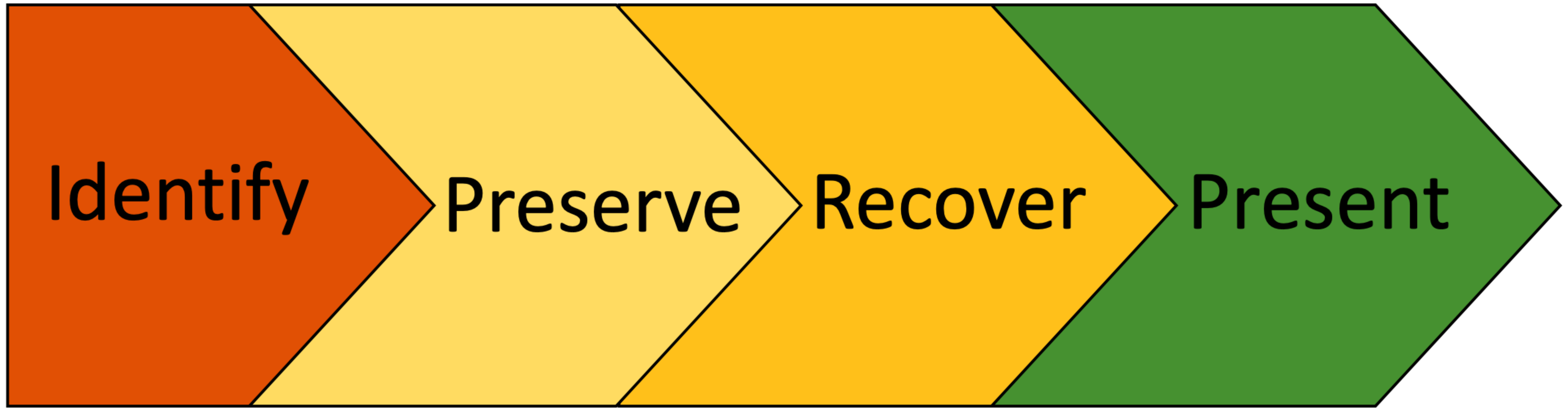
‘When forensic examiners concentrate on proving or disproving a specific claim, there can be a risk of confirmatory bias. To mitigate the risk, an increasing number of best practice guidelines are instructing forensic practitioners to evaluate the probability of evidence given on claim versus a given alternative claim.’

  - Collie (2018).

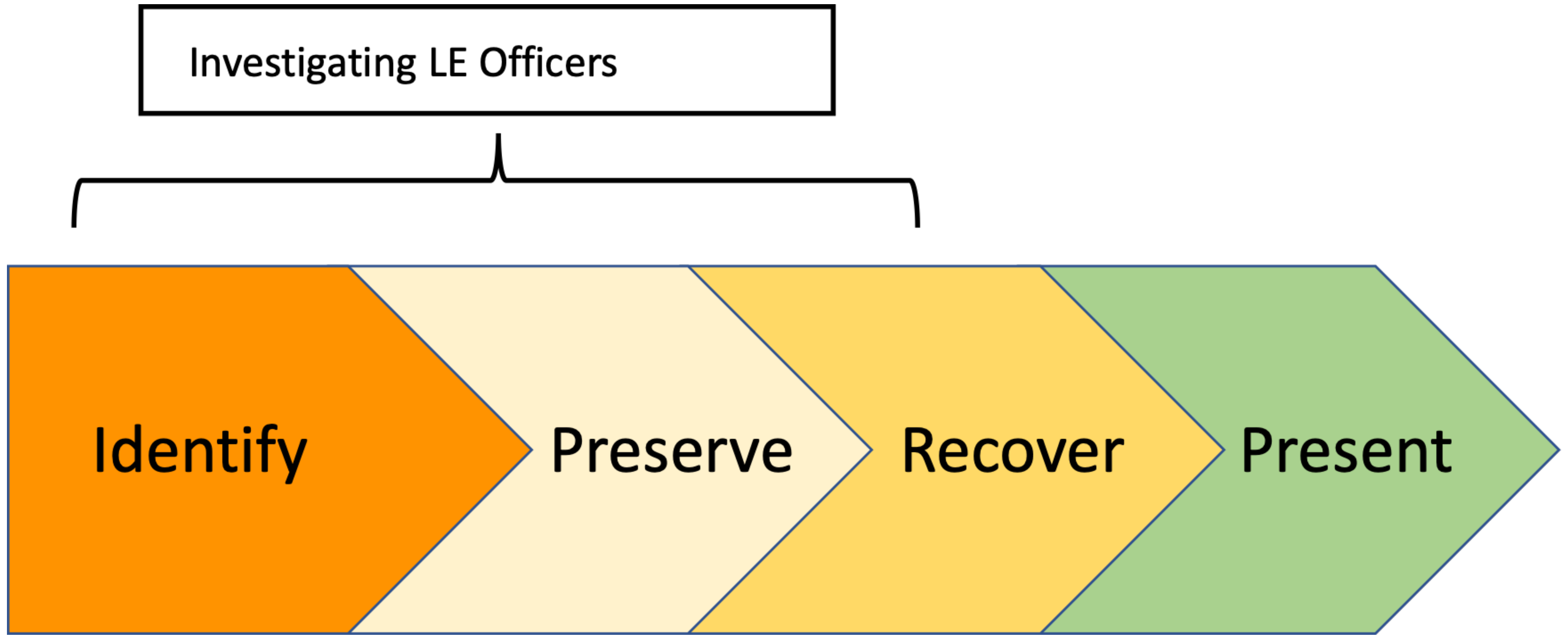
Officers may ‘cherry pick’ parts of outputs obtained from e.g. mobile phones to suit the charges made against a defendant.

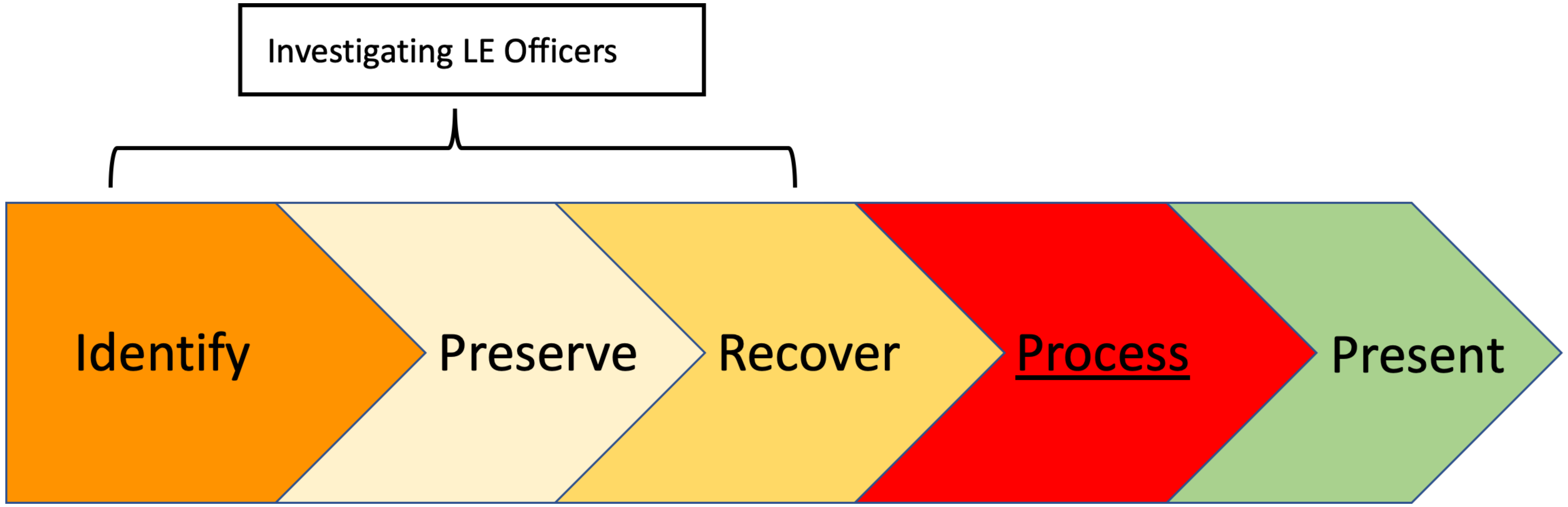
The Forensic Process

- Digital Forensic Process Model (DFPM)

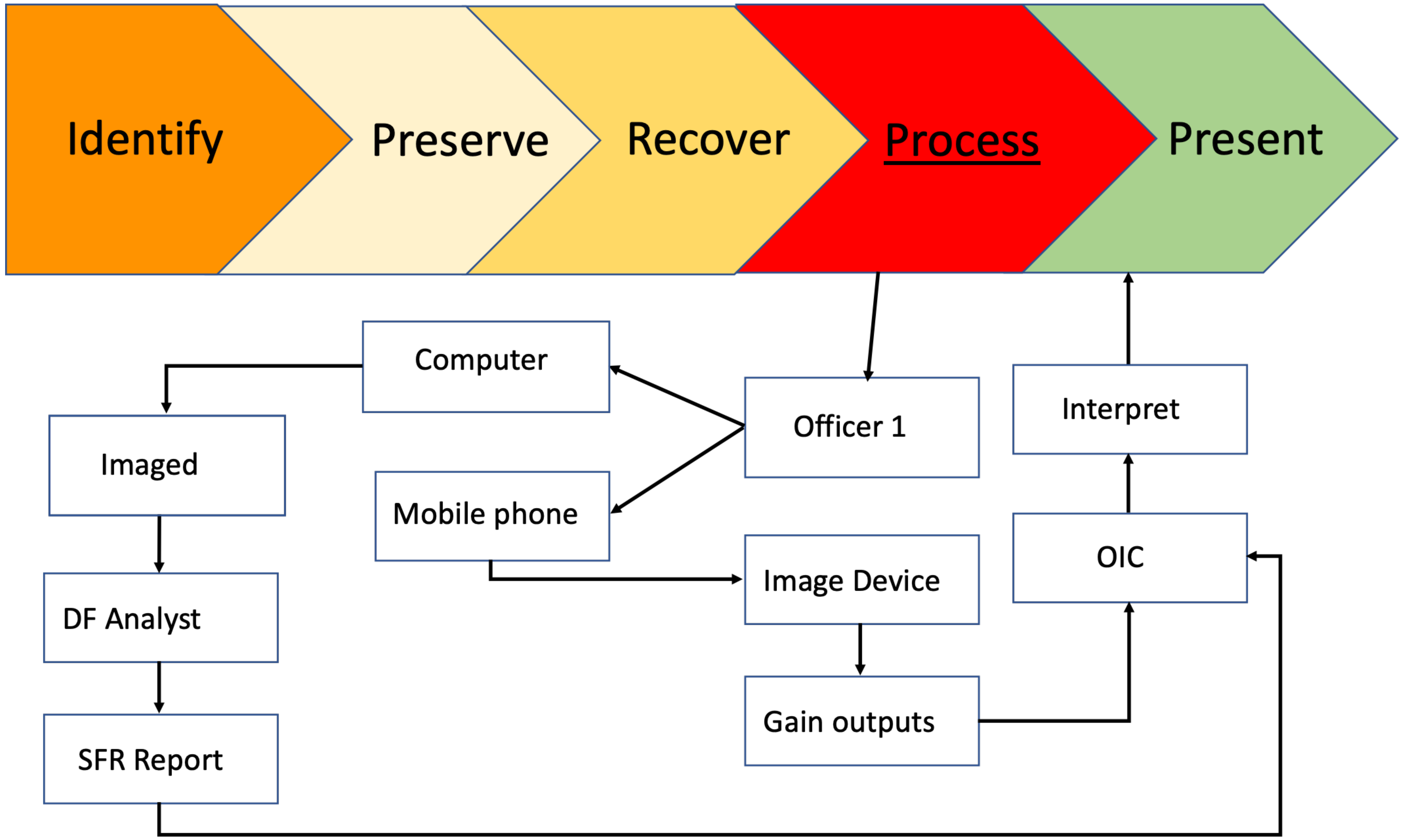


DFPM (Enhanced)



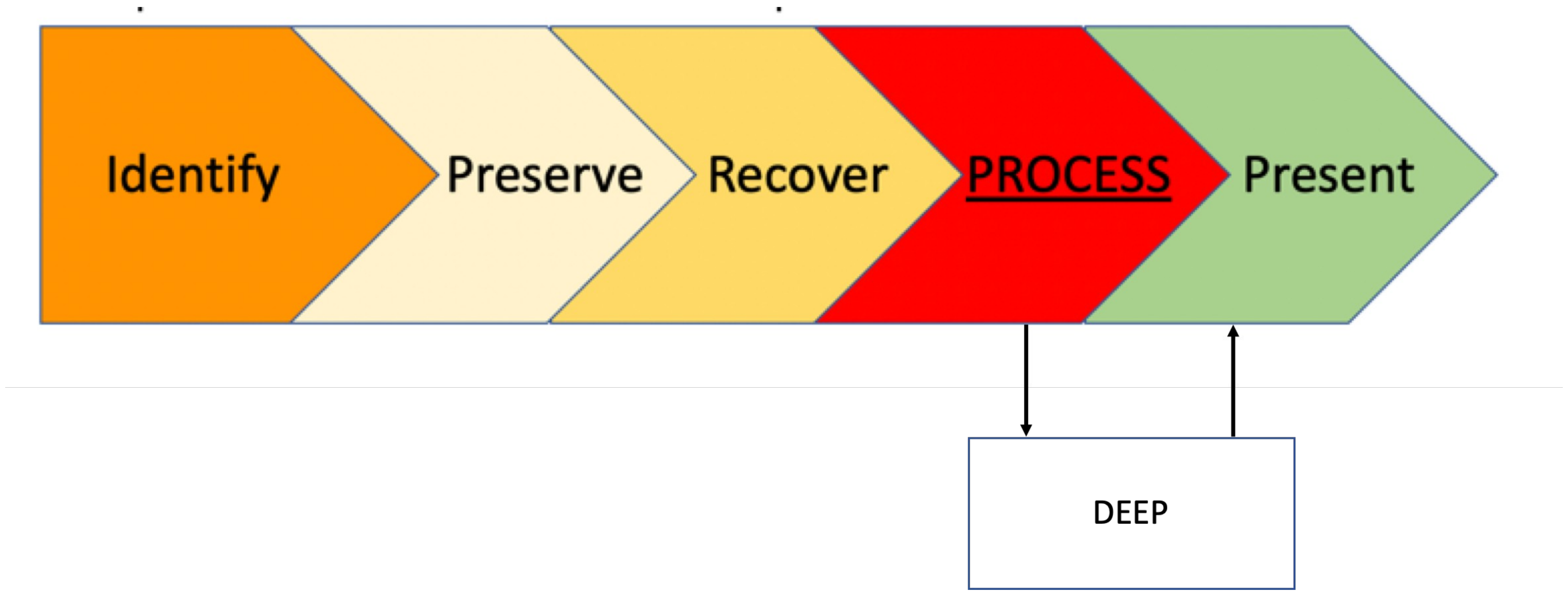


DFPM - The knowledge gap

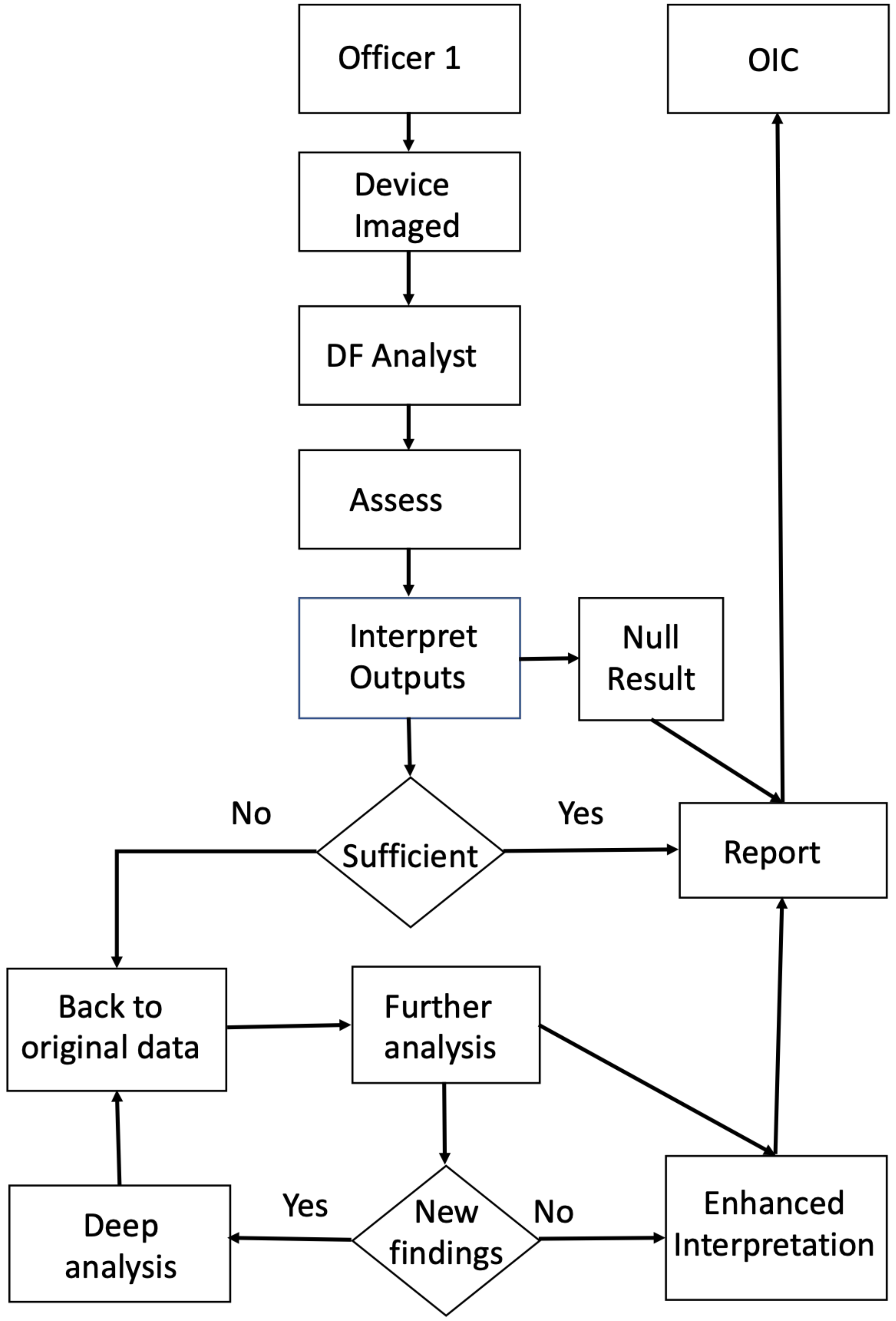


DEEP

- Digital Evidence Enhanced Process



DEEP


Officer 1
OIC
Device Imaged
DF Analyst
Assess
Interpret Outputs
Null Result
No
Sufficient
Yes
Report
Back to original data
Further analysis
Yes
New findings
No
Deep analysis
Enhanced Interpretation

References

Casey, E., 2019: The chequered past and risky future of digital forensics, Australian Journal of Forensic Sciences, DOI: 10.1080/00450618.2018.1554090.

Casey, E., 2018. Clearly conveying digital forensic results. Digit. Invest. 24, 1-3.

Collie, J., 2018. Digital forensic evidence - Flaws in the criminal justice system. Forensic Sci. Int. 289, 154 – 155. DOI: 10.1016/j.forsciint.2018.05.014

Justice Committee. Disclosure of evidence in criminal cases, HC859, 2018. Questions 173– 217. Available from:

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/oral/83096.html#

Science and Technology Committee. 2018. Oral evidence. Questions 123-131. Available from:

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html

Shaw, A., Browne, A., 2013. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digit. Invest. 10. 116 – 128.

Thank you

- Any questions?