Journal of Cyber Forensics and Advanced Threat Investigations

CFATI OPEN ACCESS

Volume 1(1-3), 42-46. https://doi.org/10.46386/ijcfati.v1i1-3.15

# The Importance Of The Three P's In The Investigation

John William Walker[1]

**Abstract**

This article introduces the importance of process during the investigation and the acquisition phases of logical/physical artifacts which may be required during the course of such professional engagement. The article then focuses on the necessity to have a robust supportive framework in a state of preparedness to facilitate the First Responders and CSIRT (Computer Security Incident Response Team) with the necessary underpin to support such investigative engagements – considering effective and pragmatic Policies, Case Management, operational Security Protocols (Run-Books) and all other necessary attributes to underpin a professional, prepared posture from which a team may effectively, and robustly engage an investigation/incident. To elaborate on the importance of such an approach, we outline a number of real-world cases where ineffective processes and controls were applied. Finally, we review the essential elements of securely managing case-related data, and the absolute need to apply security mechanisms such as Certified Standards of FIPS-140-2 encryption to secure sensitive case related assets to assure they are robustly protected at all stages of their life cycle when they are in physical transit, or when they are at rest, associated with a desk-bound PC. The end objective to the entire article is to stress an absolute need to apply process to, as far as is practicable, to achieve positive conclusions from any investigation or incident which has been engaged.

**Notes for Research**

- It has been observed from a selection of real-world cases that have either failed or been discredited by the test of challenge that the element of negligent and ineffective application of robust process was a prime contributory factor impacting with a negative conclusion to the case.
- That the lack of a robust profile of preparedness to support the First Responder or CSIRT can manifest with negative impacts on the investigation, and other associated activities such as the acquisition of artifacts. This can then amount to an inconsistent approach with engagements across the various team members, and a lack of process with applying a consistent approach with various tools (e.g. Disk Imaging).
- Whilst some First Responder and CSIRT's are accommodated with up-to-date tool-sets and applications, it is a common discovery that application/tool-related training is not included in the procurement, thus anticipating the team will learn on the job.
- It has been observed that First Responders and CSIRT members have demonstrated limited awareness or understanding of Laws, Legislation, and Standards which they should be following and applying when engaging, or discovering suggestive, implicit evidential materials.
- An exposure has been observed within a sample of investigation engagements with the application of applying robust levels of security or encryption to sensitive case-related materials and artifacts, along with an inconsistent approach when it comes to how they are processed, leaving such case related materials exposed to the potential of unauthorised access, compromise, alteration and corruption.

**Keywords**
cybersecurity, digital forensics, incident response, DFIR.

**Submitted: 14**/05/2020 — **Accepted: 10**/08/2020 — **Published: 15**/02/2021

*Corresponding author [1] Address: School of Science & Technology,Nottingham Trent University, 50 Shakespeare St, Nottingham NG1 4FQ*

## 1. Introduction

In the last decade I have acted as an Expert Witness for UK Courts, and along the way have developed and delivered specialised

Digital Forensics and Cyber Security/OSINT (Open Source Intelligence) Training to organisations such as the Saudi Arabian Ministry of Defence (MOD) located in Riyadh, the Malaysian Military Academy in Kuala Lumpur, Commercials based in Pakistan, Government and Telecommunications Agencies located in Dubai and Abu Dhabi, and to multiples of individuals across the Middle East. In this time, I have also engaged many organisations in the UK where I have worked and consulted for Oil & Gas, Betting Agencies, Government, Parliament, and a number of start-up Challenger Banks – so I wish to stress that my comments and observations within this article are not from imagination, or the work of others published on the Internet, but are based on practical, first-person hands-on experience.

As this is the first copy publication of the 'International Journal of Cyber Forensics and Advanced Threat Investigations' (CFATI) I felt it important to set the scene from which we will move forward with our future issues, and so the importance of what I call the Three P's would seem to fit very well in this inaugural launch edition. To elaborate, when I have engaged with investigations or conducted a discovery, the Three P's are the first elements I consider and apply; and when I have delivered the specialised training I introduced in the above paragraph, I always stress the importance of the application of the Three P's on day one of the training, but just what are the Three P's?

The Three P's are the most important aspects and bedrock of any Digital Forensics or Physical Investigations activity, and represent the blue line to be followed and applied at all stages to assure, as far as is practicable, the outcome of the engagement is robust and strong enough to sustain any challenge that may be presented along its path – the Three P's are the application of Process, Process, and finally Process. To exemplify this with both logic and out of real-world case management, imagine you have been leading an inter-organisation sensitive investigation which along its path takes an unexpected turn toward implications of criminality. Suddenly the entire impetus and focus of the case changes its profile, with the high probability of externals entering the logical/physical crime scene – and then when preparing the handover of the acquired, valuable artifacts, you discover that due diligence and process has not been robustly applied, implying that the value of the evidential materials are flawed at the point of acquisition through lack of applied process - for example from some real-world cases I have observed:

- The Betting Agency who were preparing a case for Court, but had not processed the Best Evidence assets correctly, and had failed to account for the asset by process of Chain-of-Custody, and to make the situation worse, had not documented the acquisition process.
- A well-known outsourcing company based in the West Midlands who support UK Government contracts– who had stumbled upon a case where paedophilic images were discovered. Here the First Responder failed to appreciate the gravity of the find, and the associated legal handling implications. Thus, they themselves were committing acts of a potential criminal nature as their expert team blundered through the investigation. To make matters worse, this discovery was not reported to Law Enforcement in accord with the related legal and ethical obligations.
- The Nottingham based Financial Services organisation who treated images of a paedophile nature as porn, applying no process or discrimination, and handling then in a manner obtuse to the implicated legal requirements.
- The Detroit based auto-mobile company who have a production plant based in West Germany. Here they discovered a server had been attached to their internal network which was feeding connection to an external community with an interest in child-related images. Never acted on correctly, never documented, and simply hidden away as dirty washing – with all perpetrators escaping the hands of law enforcement to go on and act with impunity.
- The First Responder who engaged a digital scene of crime with a technological approach – acquiring images of hard drives from a windows-based machine, not applying any robust process with no write blocking in place, and zero documentation being maintained during the acquisition process.

## 2. The Three P's

The last example of bad habits and not applying any recognised process concerns the actual acquired data, and any related dynamic digital artifacts. Here, the attending First Responder failed to recognise the need to assure that case related, sensitive data and materials should be robustly accommodated with both logical protection, and access control to the case related content. However, when tested it was discovered that such sensitive case assets had been stored on an open, shared network drive to which multiple users had either direct, or indirect access (including all Help Desk Operatives) in an unprotected folder (Hassan & Hijazi, 2017), and were no form of encryption had been applied.

To further elaborate on the aforementioned shortfalls of not following process (The Three P's), a lawyer once told me 'Most of these types of cases that fail in court, fall to the lack of any process being applied which were (are) exposed by a legal challenge of enquiry. In fact, to concur with this comment, I can add that the easiest thing to do when challenging any presented materials or artifacts is to look for the break-in process, and then to work at it to place doubt on what is being offered as case supportive evidential materials.

To accomplish the objectives of the Three P's approach, we need to have our toolkit in a state of preparedness at the outset by provisioning this important resource with the basics that must always be in place to support the First Responder and CSIRT at the outset of an engagement. Thus, below I introduce some of the most basic areas we must ensure are in place to accommodate our Three P's Framework (See Fig 1) with the robustness dictated by all engagements we encounter.

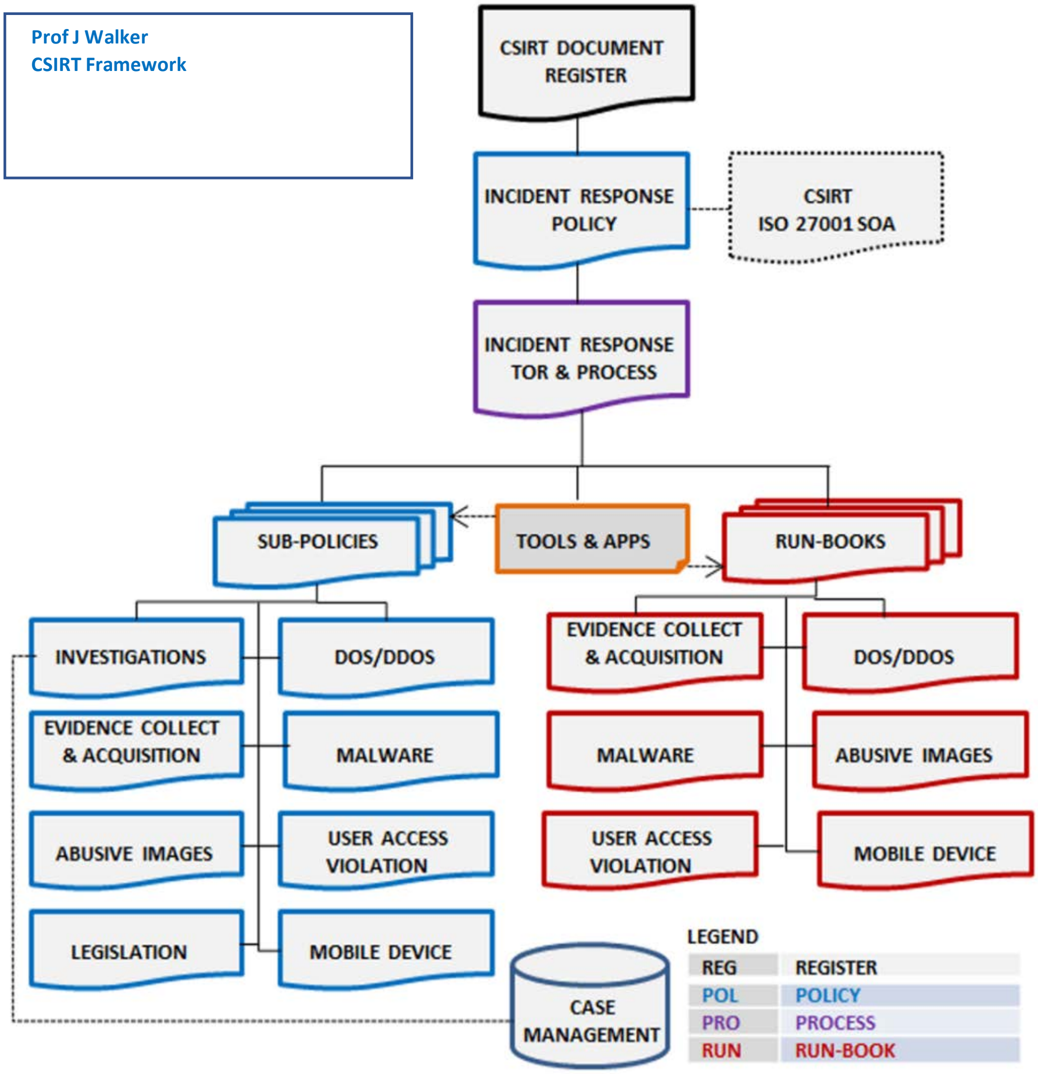


**Figure 1.** CSIRT Framework

## 2.1. Policies

Clearly, so deliver a robust structure it is essential that workable policies and pragmatic are produced and delivered to underpin and direct the team's interaction with the events they may be anticipated to encounter which are then of course associated with all the other inter-framework instruments.

## 2.2. Documentation/Forms

At the start of any engagement it is essential that the process game plan is put in place, and as such based on a recognised approach to follow well-trodden and established engagement protocols or Run-Books such as ("Enisa - CSIRT'S in Europe,") which may be shared with, say all members of the CSIRT. For example, the example Protocols as introduced below:

- **Acquisition of Artifacts** : including direction on the chain-of-custody process, bag, tagging and recording of acquired evidential materials (Officers, 2012).
- **Image Acquisition:** The process of extracting and image from a computer, outlining the areas where and how write blocking should be applied (or not), and how such acquired images should be managed – how many copies should be taken, and how they should be allocated hashing to demonstrate in the future they have not been corrupted, altered or tampered with.
- **Handling of Physical Artifacts:** The process around the handling and processing of physical assets where bio cross-contamination could take place.

### 2.3. Laws and Legislations

It is of paramount importance that all engagement follows the applicable, mandated laws, legislations specific to the global location or locations, and where required as applicable the obligated standard (e.g. PCI-DSS). For further example the legal obligations when dealing with child images of a sensitive nature falling under the classification of the COPINE scale (Database) (Combating Paedophile Information Networks in Europe) which is used to distinguish between child erotica, and pornography.

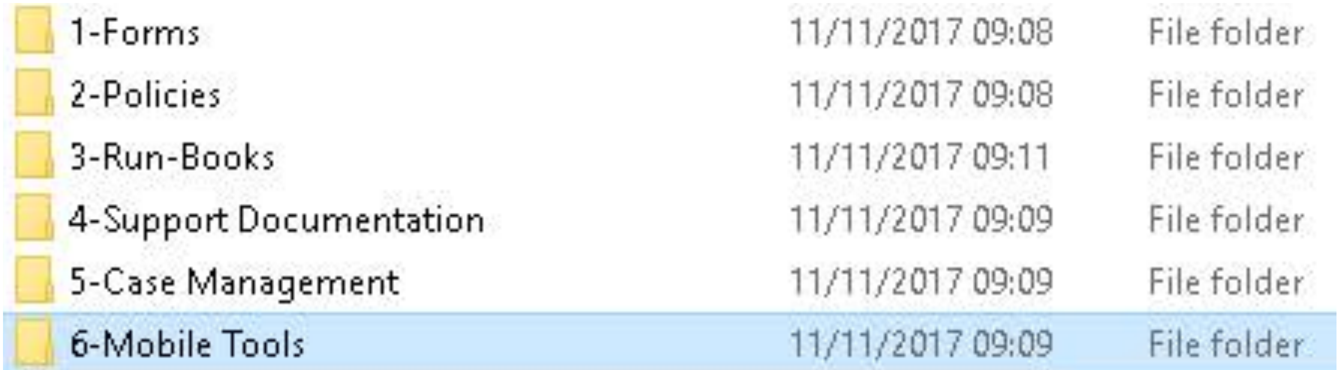
### 2.4. Tools and Training

It is of course essential that the team are accommodated with up-to-data tools and applications to carry out their duties within the parameters of the team's limitations - but it is also equally important to remember that such tools need to have trained operatives driving them, so be sure that training is accommodated into the cost of procurement for all team members who may be required to use them ("College of Policing – Digital and Cyber Crime,").

### 2.5. Secure Handling of Data and Logical Artifacts

Over the years of my operational career I have observed many unacceptable, bad practices committed during the process of an investigation which left sensitive data open to unauthorised and unknown access, abuse, compromise, and the potential of illicit alteration. Actions of which not only impact the case related materials, but negligence which left submission of any such evidential material wide open to challenge. My approach here, and recommendation to all is to always use a trusted secure encrypted drive when travelling, or on occasion when at a fixed desk-bound PC. The advantages are multiple, as minimum ranging from assuring that the acquired materials are safe and under robust access control, that they are secured by a FIPS-140/4 certified level of encryption (Wikipedia), which allow the data custodian of the evidential assets to testify they have, at all times been maintained under robust and controlled secure custody. Also, if such a sensitive asset is lost or stolen its content may be considered secure as such the device is facilitated with an approved pin access control mechanism which will self-destruct the logical content after multiple incorrect pin sequences are entered to access the content.

In my case to accomplish these areas, as part of my Three P's process I always use the iStorage (iStorage) diskAshur Pro for my mobile activities as a CSIRT on a drive – See Fig 2 below, and the larger desk-bound diskAshur DT as a more permanent of PC associated facility to secure my case related materials and case backups.



| | | |
|---|---|---|
| 1-Forms | 11/11/2017 09:08 | File folder |
| 2-Policies | 11/11/2017 09:08 | File folder |
| 3-Run-Books | 11/11/2017 09:11 | File folder |
| 4-Support Documentation | 11/11/2017 09:09 | File folder |
| 5-Case Management | 11/11/2017 09:09 | File folder |
| 6-Mobile Tools | 11/11/2017 09:09 | File folder |

**Figure 2.** Travelling First Responder CSIRT

## 3. Conclusion

It is sadly a case that a selection of responders can be very proficient when it comes to using the latest and greatest digital forensics tool to speedily grab, say the necessary image from a PC drive, or to acquire the contents of a seized cell phone. However, it is the seasoned, process aware professional who can accomplish the same tasks, but in a manner, which will accommodate a test or challenge – a professional who will apply the required levels of process and due diligence to deliver a robustly sound investigation conclusion - as opposed to one which may be found wanting at some inopportune time. As I said at the start, and as I comment in this conclusion, the three most important bedrock aspect of any case are process, process, and yes you guessed it, process.

## Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) declared no financial support for the research, authorship, and/or publication of this article. Or please insert other relevant information here.

## Acknowledgments

To the creators of DFIR Tools and Run-Books.

## References

College of Policing – Digital and Cyber Crime. Retrieved from https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx

Database, U. a. I. UK and Ireland Database COPINE Scale. https://theukdatabase.net/uk-child-abusers-named-and-shamed/childhood-abuses/paedophile-party-members/

Enisa - CSIRT'S in Europe. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe

Hassan, N., & Hijazi, R. (2017). Digital Privacy and Security Using Windows: A Practical Guide: Apress. DOI : 10.1007/978-1-4842-2799-2

iStorage. Encrypted Drives. Retrieved from https://istorage-uk.com/product/diskashur-pro2/

Officers, A. o. C. P. (2012). ACPO - Good Practice Guide for Digital Evidence. Retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Wikipedia. FIPS 140/2. Retrieved from https://en.wikipedia.org/wiki/FIPS_140-2