Annual ADFSL Conference on Digital Forensics, Security and Law 2017

May 16th, 3:15 PM

Case Study: A New Method for Investigating Crimes Against Children

Hallstein Asheim Hansen
Norwegian Police, hallstein.asheim.hansen@politiet.no

Stig Andersen
Norwegian Police, Stig.Anderson@politiet.no

Stefan Axelsson
Norwegian University of Science and Technology, stefan.axelsson@ntnu.no

Svein Hopland
Norwegian Police, Svein.Hopland@politiet.no

CASE STUDY: A NEW METHOD FOR INVESTIGATING CRIMES AGAINST CHILDREN

Hallstein A. Hansen[1], Stig Andersen[1,2], Stefan Axelsson[2], and Svein Hopland[1]

[1]Norwegian Police, Oslo Police District
[2]Norwegian University of Science and Technology (NTNU)
{Hallstein.Asheim.Hansen, Stig.Andersen, Svein.Hopland}@politiet.no,
Stefan.Axelsson@ntnu.no

ABSTRACT

Investigations of crimes against children are often complex, both in terms of the varied and large amount of digital technology encountered and the offensive nature of the crimes. Such cases are numerous, large, and prioritised, requiring digital forensics competence. Earlier digital forensics was considered and treated as a typical forensic science like fingerprint analysis, performed in a laboratory isolated from the investigative team. This decoupled way of working has proved to be both inefficient and error prone.
At the Digital Forensic Unit of Oslo Police District we have developed a new way of working that addresses many of the problems created by the earlier lack of integration. This method stresses a much closer co-operation between the digital and criminal investigators. We document this method and share our experiences, hoping to spur more discussion of specific methods for dealing with particular types of cases with a large digital component.

Keywords: Process and procedures, techniques and tools, cyber crime investigations, law enforcement, crimes against children

1. INTRODUCTION

As a rule modern criminal investigations involve digital evidence, whether a single cell phone or video surveillance installation, or numerous devices from various sources and of different types. Crimes against children, including child abuse and sharing child abuse material, is a category of offense where digital evidence is often prevalent. Perpetrators tend to leave behind digital evidence even when committing physical offenses, e.g., photos and videos.

Law enforcement agencies must develop a suitable working method for investigating these crimes, including the Oslo Police District where three of the paper's authors practice digital forensics. Typically, a law en-

forcement agency splits case work on crimes against children between a Sexual Crimes Unit and a Digital Forensics Unit.

In our organization the Sexual Crimes Unit would traditionally request assistance from the Digital Forensics Unit to, for example, participate in search and seizure operations, acquire digital evidence from devices, or analyze digital evidence.

Communication would follow the example set by how law enforcement interacts with most other forensic sciences, such as fingerprint analysis. The request for assistance was formulated in writing and the end result returned: Evidence files, artifacts from the digital evidence, and a written report. Sometimes this was the complete extent of communication between criminal and digital investigator.

There is traditionally a debate between those that view digital forensics as mainly a traditional laboratory science and those that view it more as an investigative tool. While this debate is still not settled, we agree that digital forensics, due to the required specialist training, methods, and equipment, coupled with the pervasiveness of digital data, occupies a middle ground between the two perspectives. Indeed, the digital realm may be a crime scene (a computer, web site, etc.), evidence (documents, system logs, etc.), or the means of carrying out a crime, (malware, a phishing site, etc.) [7].

While other forensic disciplines feel their quality is best assured by "hiding in the lab", knowing as little as is practical about the actual case to remain unbiased, we are sceptical of this approach in general. Data must be interpreted in context, which the case provides.

We believe forensic accounting is a better model for digital forensics. Forensic accounting is applied in criminal investigations involving, for example, bankruptcies, narcotics, tax fraud, money laundering, trafficking, etc. The practitioners typically have a background from finance or auditing. Interpretation, presentation, and assessment of financial records require the forensics accountant to be immersed in the case details.

We also side with the idea of close cooperation from a purely practical perspective, e.g., restraints on time and other resources. We need to work closely with the criminal investigator to be able to prioritize work and correctly interpret its impact on the investigation at hand, as and when results become available.

Our Digital Forensics Unit is continually working to improve collaboration, communication, and knowledge sharing with other Departments. This integration is tightest between the Digital Forensics Unit and the Sexual Crimes Unit in work on crimes against children. This is due to the often huge amounts of data involved and the precautions the perpetrators typically take to avoid being detected and successfully investigated. Investigation efficiency and quality has improved so much that we now speak of an entirely new method for investigating crimes against children.

This new method focuses on tight integration between Sexual Crimes Unit and Digital Forensics Unit management, and between the criminal and digital investigators. There is an emphasis on better communication, collaboration, and knowledge sharing. Triage [2] is employed as a crucial tool in the early stages of an investigation.

Our main contribution in this paper is to highlight the need to integrate digital investigators in the investigation from the start. We report qualitatively on our experiences of having worked in this manner over time in a fairly large organisation. This in the hope

that other practitioners will be inspired to do the same and so build a more substantial and quantitative body of knowledge for approaching these types of investigations.

2. RELATED WORK

The current state of the trends in digital forensics when it comes to case sizes, etc. has been empirically studied. Irons et.al. [5] studied how the volume of case material and number of cases have grown between 2007–2011 using data from the FBI. In the period in question the average size (in bytes) per case has doubled, and the complexity (number of sources, diversity etc.) has also increased.

There is little concrete information in the research literature on how digital forensics units are usually organised and work. Gogolin [4] discussed overall readiness and the types of cases that faced US law enforcement, especially in Michigan, concluding that the outlook was bleak. We infer from the data presented that, as in most other cases we have come across, digital forensics units are organised in separate laboratories with no early and natural connection to the investigation as a whole.

While there is some work reported on the forensic process in general, we have not found much in the area of methods and processes for working cases with an important digital component, with two notable exceptions:

Firstly, Awadi et.al. [1], study the actual time taken to conduct investigations based on several confounding factors. The article doesn't say outright how close criminal and digital investigators work, but their study of "case detail", i.e., how much relevant case information is communicated to the digital investigators, leads us to believe that their organisation is a more traditional one. They support the hypothesis that the more information the digital investigator is given, the less time they need to work the case, which agrees with our observations from changing to a more integrated method.

Secondly, Casey et.al. [3], point out that traditional forensic process descriptions put undue emphasis on individual tasks in isolation. They argue for a more integrated approach where the digital investigator becomes part of the decision making process. They note that tools currently do not support working in this way as well as they could (and should). The types of tasks they describe is not divided by type of crime, but rather type of digital investigation task such as malware analysis or network forensics, compared to our crime-centered approach.

A literature review would not be complete without mention of *triage* [2], traditionally viewed mainly as an answer to the problem of being overwhelmed by the amount of data to analyse. However, deciding what to analyse means deciding which information could be pertinent to the investigation. This is a decision making process uncomfortable to those that view digital forensics less as an investigative tool and more as a laboratory science. We, on the other hand, see the need for close cooperation between digital forensics and the investigation. Hence triage is more a result of that cooperation, not its entry point. This is supported by Casey [2]: "The debate over whether digital forensics is an investigative tool or a scientific discipline is a false dichotomy: it is both. Performed prudently, triage is the perfect manifestation of this duality of digital forensics, providing useful information in a timely and cost effective manner while maintaining the forensic soundness of the evidence to support decision makers in battlefields, boardrooms, and courts." This paper is our attempt at de-

scribing how this process works in our particular circumstances.

Casey's statement notwithstanding, much of the literature does not take this view. Instead the triage decision of what is useful to the investigation is made implicitly, based on some model of what has usually been the case.

3. OLD METHOD OF INVESTIGATING CRIMES AGAINST CHILDREN

We present some of the characteristics of our law enforcement agency and our way of investigating crimes against children before we developed our new method, and typical undesirable consequences from applying the old method.

3.1 Oslo Police Department

Oslo Police Department has around 3000 employees, of which 2000 work directly in law enforcement. It serves the Norwegian capital and so often investigates the country's most severe crimes. It is at the leading edge of law enforcement methodology in our nation.

The Sexual Crimes Unit employs 100 investigators with police backgrounds, and investigates crimes such as rape and sexual harassment in addition to crimes against children.

The Digital Forensics Unit is split 50/50 between investigators with police backgrounds and investigators with computer science backgrounds. It has grown from 5 people in 2006 to around 30 people in 2017. During this time both the volume, diversity, and complexity of digital evidence and their carriers, e.g., computers, phones, and the Internet, have increased dramatically. There is no indication that this trend will abate.

Additional challenges to integration is caused by the Sexual Crimes Unit and Digital Forensics Unit being separated both organizationally and by location. This division has become more pronounced as the need to collaborate on investigating crimes against children have become more urgent over the years.

3.2 Method description

The method of investigating crimes against children in our organization has never been static. While we present the 'old' and 'new' methods, we ask the reader to bear in mind that the method has been continually developed, executed, and evaluated over the recent years. The old method presented here represents the methodological challenges we have encountered and worked to overcome. The new method presented in the next section represents a cumulative best practice, not the result of a sudden change.

In our experience investigative methods are applied iteratively and evaluated after each iteration. When investigating crimes against children, an iteration typically has the following phases (Figure 1):

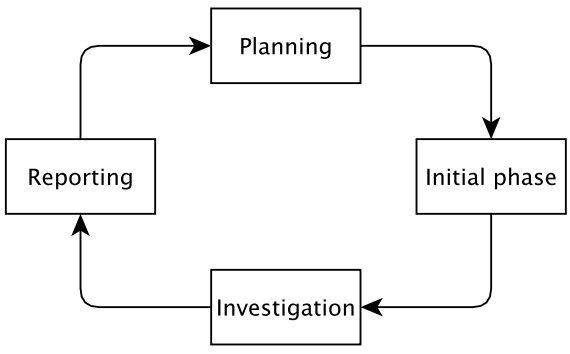

Figure 1. The investigation phases

- Planning: The investigation is prepared.
- Initial phase: A time-constrained, resource intensive, crucial stage of the investigation aimed at identifying and apprehending all suspects and gaining control of relevant evidence items through search and seizure operations.
- Investigation: The major investigative work.
- Reporting: Official documents are written, court testimonies given, and the iteration evaluated, influencing which further investigative methods to apply.

The all-encompassing challenge to the investigation of crimes against children at our organization was that the Sexual Crimes Unit saw investigations as internal matters. The Digital Forensics Unit would be limited to performing isolated, technical tasks, with little or no knowledge of the case in question.

For illustration purposes we present an example of the investigation of such a (hypothetical) case. As noted we continuously work to improve our methods and organization, so the example below will not be based on any particular investigation, but rather demonstrate a worst-case scenario.

Example: Case and preliminary investigations

> The police receive a report from a local water park. A man in his forties has filmed children bathing using a concealed camera. The man has been identified.
>
> The Sexual Crimes Unit performs a preliminary investigation: The water park attendant who reported the issue is interviewed, and the suspect is looked up in available databases.
>
> The suspect has no criminal record, but an earlier report states he has been observing children in a kindergarten. He is a computer engineer who works as a system administrator, is married, and has two young daughters.

3.3 The planning phase

The Sexual Crimes Unit would plan traditional investigative steps: Apprehending and interviewing the suspect, searching his/her home and office, and seizing any relevant items found, phones and computers included. No other technical preparations, nor any effort to gauge the technical skills of the suspect, would be made. Neither the head of the Sexual Crimes Unit nor the case's principal investigator approached the Digital Forensics Unit.

Example: The Planning phase

> The Sexual Crimes Unit makes plans to apprehend the suspect, search his home and seize relevant evidence items. The assumed computer skills of the suspect is noted, but the hypothesis that he may have molested his own children causes the greatest concern. With respect to electronic evidence, a thorough search for a 'spy camera' is to be conducted. The police officers are also instructed to seize the computers the suspect seems to use the most, since he may have more than one. The Digital Forensics Unit is not notified.
>
> Since the planning stage does not involve the Digital Forensics

Unit, their administration cannot provide any input, such as suggesting that the suspect's computer skills are taken into greater consideration, and that a team of digital investigators participate in the search.

3.4 The initial phase

The subject would be apprehended, but no technical questions put to him. Unlocked phones and computers might be summarily searched without documentation or use of digital forensic tools. Running computers were seized according to the, often lacking, experience and routines of the Sexual Crimes law enforcement officers.

If the officers on site deemed that technical assistance was required, they would contact their principal investigator. He in turn would contact the head of the Sexual Crimes Unit who might, through the chain of command, requested assistance from the Digital Forensics Unit. A substantial delay was introduced whether digital investigators visited the crime scene or advised by phone.

Both field work and the crucial preliminary investigative steps while the suspect is held in custody and subjected to his first interview require substantial resources. The Digital Forensics Unit management would usually have little time to allocate these resources, and the digital investigators little time to prepare.

Example: The Initial Phase

> The suspect is apprehended and asked about his spy camera and computer usage. He informs the Sexual Crimes officers where the camera is hidden, and that he mainly uses a large workstation in his home office. This is good, because his home is littered with computer equipment, a lot of it old and apparently unused. The spy camera, other cameras, his unlocked phone, and the workstation are seized. The computer is switched off and all attached peripherals are left on scene. The phone is searched manually. Nothing of interest is found.

This is a worst-case scenario: The phone is handled by the officers and no real evaluation of the computer equipment is done. We can imagine a less extreme situation where the officers call in, wondering what to do about all the computer equipment. After some time they are redirected to the Digital Forensics Unit. The digital investigator, unfamiliar with the case, might recommend bringing in all the equipment that looks recently used, as well as asking the suspect for his computer passwords and PIN code. She asks the Sexual Crimes officer to bring the phone to the Digital Forensics Unit for immediate acquisition.

3.5 The investigating phase

Earlier the Digital Forensics Unit would not be involved unless asked specifically. This was done through a form called a *Request For Assistance*, where the principal investigator specified the desired technical investigative steps.

The Request For Assistance would be sent from the principal investigator to the Sexual Crimes management for prioritization. Digital Forensics Unit management respected this prioritization and assigned a digital investigator to the case in the manner of traditional forensic sciences [6].

The digital investigator could then communicate directly with the Sexual Crimes investigator. The Request For Assistance

would be adjusted and sometimes completely changed due to a new, shared understanding of the case and request. When the task was completed the digital investigator took no further part in the investigation unless more investigative steps were requested.

Example: The Investigation Phase

> The investigation first focuses on interviewing the suspect's family. Luckily, there are no indications of him molesting his two daughters. The only cause for concern is the contents of the spy camera. It contains hundreds of pictures and videos, almost exclusively of young boys.
>
> After some days or weeks the Sexual Crimes Unit sends the computer to the Digital Forensics Unit just to 'be on the safe side' before the police prosecutor merely charges the suspect with a 'filming without consent' offence.
>
> The computer appears to runs Linux and to contain encrypted hard drives. Sexual Crimes asks the suspect for his password, but he refuses, citing trauma from his experiences and invasion of his privacy. The principal investigator asks the Digital Forensics Unit not to spend resources to try to gain access to the data on the computer.

3.6 The reporting phase

Earlier the Sexual Crimes investigator and digital investigator wrote independent reports. Either the Sexual Crimes investigator would use the digital investigator's technical report as part of his testimony, or the digital investigator would be called to testify, basing her testimony entirely on her own report. Work on the case was independently terminated by Sexual Crimes and Digital Forensics Unit, frequently leading to wasted effort.

Example: The Reporting Phase

> The Sexual Crimes investigators report on their examination of the suspect's phone and spy camera. The latter report documents the pictures and videos found and uses the time-stamps as shown by the non-forensic tool used for examination.
>
> The digital investigator reports on her successful acquisition of the computer hard disks and failed attempt to decrypt the data.
>
> The suspect pleads guilty to filming without consent and receives a suspended sentence.
>
> Should the case go to court, the digital investigator might not be called upon to testify. A Sexual Crimes investigator simply informs the court that the suspect's computer appears to be encrypted.

It should be clear from our example that the main challenge facing the investigation was the lack of the required knowledge to make right decisions. This was caused by lack of communication and an organization that would have facilitated it. The competence existed, but was just not used correctly. The old method is illustrated in Figure 2

We will revisit the example when we evaluate the new organization below.

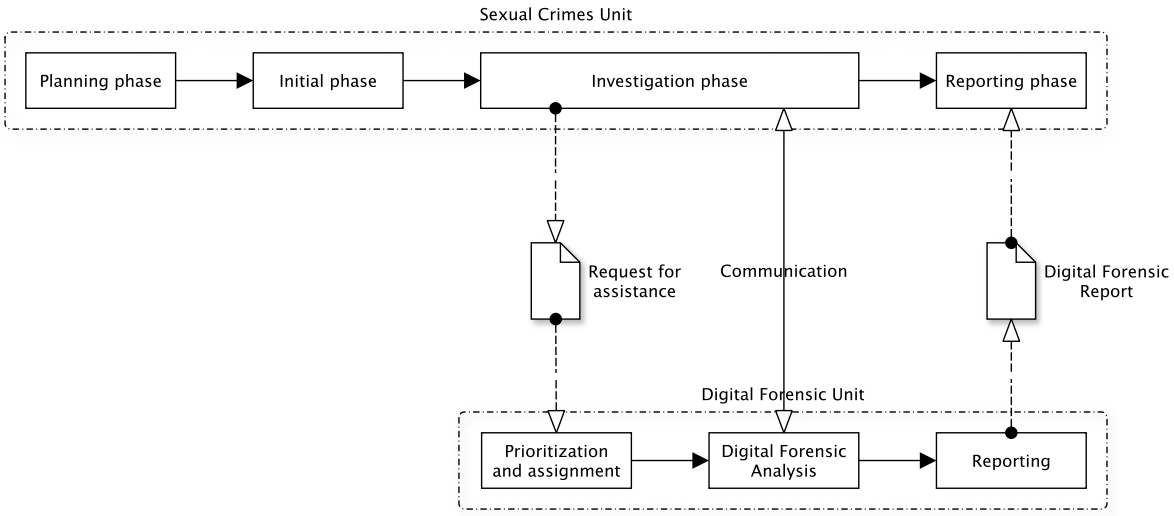

Figure 2. Old method

4. NEW METHOD OF INVESTIGATING CHILD ABUSE CASES

The challenges presented above were often easy to spot but nontrivial to remedy. The established culture and inertia of the organization required significant efforts to overcome.

It was the persistence of key individuals at the Digital Forensics Unit and Sexual Crimes Unit and recognition at the management level that made possible a permanent change for the better. Though as noted, this is, and will always be, ongoing work.

The Sexual Crimes Unit has created a group of criminal investigators dedicated to digital investigation of crimes against children. Its members have greater understanding and knowledge of digital forensics than the average criminal investigator. The group leader is the point-of-contact with the Digital Forensics Unit. The Digital Forensics Unit helps develop this group by offering seminars, training, and assistance, as well as working through a shared case management system.

The Digital Forensics Unit has reorganized from a technical division, i.e., computer and mobile forensics, into four groups divided by crime type: Homicide, Computer Crime, Fraud and Narcotics, and Sexual Crimes [8]. The leader of the latter is the point-of-contact with the Sexual Crimes Unit. The digital investigators of this group have experience working crimes against children, and are able to understand the requirements of the criminal investigators.

Below we describe our new method. Note that all the primary changes deal with organization, communication, and the application of knowledge. The introduction of new tools and techniques, while important in themselves, is secondary. In our experience, the quality of work in any phase is crucial in ensuring the success of the following phases. The iterative nature of criminal investigations creates a chain of such dependencies.

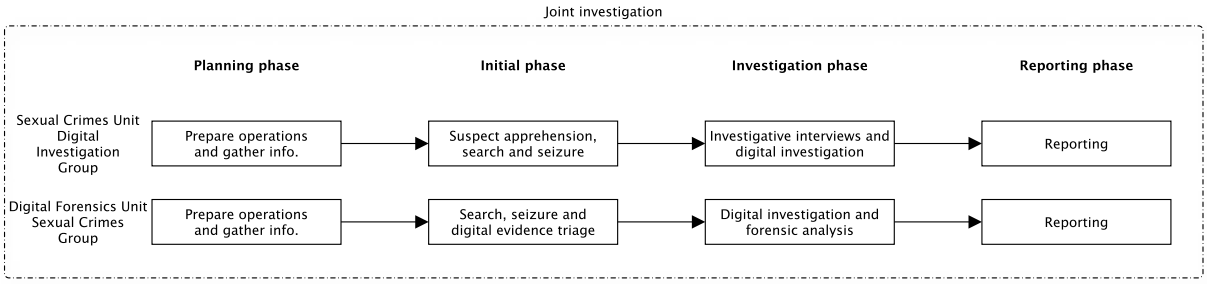

Figure 3. New method

4.1 Planning phase

Significantly, before planning a police operation, the Sexual Crimes administration now considers involving the Digital Forensics Unit whenever a new, relevant investigative step is taken. The Digital Forensics Unit may be involved in the planning, asked to provide personnel for the police operation, or merely to advise over telephone, depending on the perceived need.

The Digital Forensics Unit, management and digital investigators alike, are given the chance to: Influence the plan; prep the Sexual Crimes investigators, e.g. to ask suspects for passwords and PIN codes; and to assign the right digital investigators to the police operation and give them time to prepare equipment and rehearse routines appropriately.

Example: The Planning phase

> Following the new method, Sexual Crimes management involves the Digital Forensics Unit at the planning stage due to the presumed computer skills of the suspect.
>
> Open source intelligence reveals that the suspect is a Linux expert and digital investigators with Linux competence are assigned to the case, prepared for a complex computer setup and encryption. The criminal investigators, experienced with similar cases, assume that the suspect may share child abuse material over the Internet.

4.2 Initial phase

The initial phase focuses on competence, communication, and timeliness. Sexual Crimes and Digital Forensics Unit management has, in the planning phase, ensured that personnel with the necessary skills are available at all times and on relevant locations. A police operation often implies concurrent activities and tight coupling of information with implications for decision making. Good lines of communication are thus crucial, along with performing triage. Again, technical tools are of secondary importance.

Example: The initial phase

> The suspect is apprehended and his unlocked phone is seized by Sexual Crimes and brought to the Digital Forensics Unit. En route to the police station the suspect is questioned about his spy camera and computer usage, including his user accounts, PIN codes and

passwords. He refuses to provide these.

Later, the digital investigators arrive on scene. Criminal investigators inform that, apart from verifying that the suspect's workstation has a locked screen, they have not touched any computer equipment.

The digital investigators discover what seems to be file servers, external hard drives, and USB drives. Unsure of what to do with the locked computer, they collect the powered-off media, previewing some through a write-blocker, including the spy camera. The camera contains mainly pictures and videos of young boys. This information is passed on to the criminal investigators about to interview the suspect. All examined external hard drives appear to be encrypted using Truecrypt full-disk encryption. Some of the USB drives also appear to be encrypted. Others contain data deemed irrelevant to the case.

Meanwhile the digital investigators at the lab have extracted data from the suspect's phone. This reveals several stored passwords, which are communicated to their colleagues at the scene.

One of the passwords unlocks the screen of the workstation, and the digital investigators acquire live data from the Linux system. A quick, documented examination of the system reveals several unmounted partitions, apparently encrypted. Truecrypt is installed. The system is shut down, and all the equipment is brought back to the Digital Forensics Unit for triage, imaging and further investigation.

During file carving one of the USB drives, a digital investigator discovers several hundred deleted images, depicting abuse of young boys. An investigator from the Sexual Crimes group evaluates the find, selecting some to be showed to the suspect, currently being interviewed.

When confronted the suspect admits to possessing the pictures and offers up the password to his encrypted drives, which is communicated to a digital investigator. She, after discovering a typo in the password, is able to decrypt several disks. They contain millions of child abuse artifacts.

The example shows how overall competence, and communication between units, provide the investigation with crucial pieces of digital evidence. These are combined with traditional investigation methods to essentially break open a case on the day of the police operation.

4.3 Investigation phase

The *Request For Assistance* form is no longer in use. Investigators from the Sexual Crimes Unit and the Digital Forensic Unit now communicate directly: In meetings and briefings, face to face, and via emails, phone, etc. The criminal investigator employs traditional law enforcement methods as well as digital forensics. In the latter case they do most of their work at the Digital Forensics Unit labs.

The digital investigator works independently or in tandem with the criminal in-

vestigator to uncover relevant evidence on the forensic images, typically multimedia, chats, and user account information. The large amount of information on all but the smallest media image requires frequent and substantial communication to avoid misdirected investigation, resulting in a broad and detailed, shared view of the case among the investigators. The criminal investigator and the prosecutor evaluate the findings and plan out the next steps of the investigation, communicating closely with the digital investigators.

On the management level each case is now evaluated and prioritized early on by representatives from both groups based on a more complete set of criteria, including severity, number of suspects and victims, complexity of digital information and the expected digital competence of the suspect(s). The prioritization is continually re-evaluated, often several times per week. This allows both teams to order and re-order their tasks based on the total, overall progress in each case. Less time is wasted waiting for information, evidence items, or results from the other group.

Example: Investigation phase

> The two groups work the case, documenting the child abuse material and the material produced by the suspect himself. His contacts in the online community of file sharers are investigated.
>
> The suspect is confronted with the digital evidence and pleads guilty. He is interviewed to investigate if physical abuse has taken place. Any downloaded child abuse material that might document ongoing abuse is followed up.

4.4 Reporting phase

Whether reporting on the case in writing or as court testimonies, both the criminal and digital investigators now share a common understanding of the case at hand. All crucial points are discussed and documented with due care. The digital investigators write reports on the relevant facts of the case in support of the reports written by the criminal investigators. Any uncertainties and ambiguities are resolved.

Example: Reporting phase

> The digital investigators document the technical details of the suspect's devices and Internet use. The criminal investigators document the analysis of the child abuse material. The police prosecutor requests further investigative steps and reports in order to build the case and support the confession of the suspect. The criminal and digital investigators plan and execute these steps together.

The two examples illustrate the interdependence of the different phases. The 'new' example takes a different route from the 'old' example from the planning phase onward. The distance only grows as the investigation progresses. See Table 1 for a comparison of the two methods.

In addition to the increased quality of the investigation, we also believe we save resources and reduce latency. The new method is illustrated in Figure 3

5. EXPERIENCES

As a result of applying the new method Oslo Police Unit is now treating cases involving sexual child abuse in a more uniform way and with increased quality [8]. In

Phase	Old Method	New Method
Planning	DFU not involved in planning	DFU involved in planning
Leads to	DFU unaware and unprepared, few technical considerations made	DFU prepared, technical challenges anticipated
Initial	Sexual Crimes unable to handle technical challenges. Digital investigator unprepared, unfamiliar with case, may be a bad match competence-wise. Collaboration and communication ad hoc	Communication and collaboration set up beforehand. Digital investigators well prepared, case-updated, with appropriate competence
Leads to	Lower quality technical work, missed crucial early opportunities	More leads found, good results produced in early investigation
Investigation	Decoupling in management, heavy form use, investigators work in isolation, work independently terminated	DFU and Sexual Crimes group leaders choose right team of investigators. Competence and case information is shared, desired leads sought.
Leads to	Time and resources wasted on misguided, excessive, or useless investigative steps. Important leads missed, potentially ones absolving suspects	Little overhead, most investigative steps justified, high chance of producing relevant leads
Reporting	Reports written independently. Tactical reports and testimonies based on wrong interpretation of digital evidence. Technical reports and testimonies decoupled from case, improperly presented for its audience	Documentation reviewed by team members if necessary, technical correctness and appropriateness ensured. Testimonies given with sufficient technical and case knowledge
Leads to	Documentation does not enlighten decision makers. Erroneous court rulings	Documentation and testimonies serve their purpose. Chance of erroneous court rulings reduced

Table 1. Comparison of old and new methods

an interview the group leader of the newly established Sexual Crimes digital investigation group claims that "the greatest result of the new way of cooperating is minimizing the possibility of miscarriages of justice due to lack of knowledge about the digital evidence."

Investigators from both groups report that the new way of cooperating allows investigators to work together on multiple consecutive cases, giving them a better understanding of the other group's work processes, challenges, and profession. They adapt the way they work to better suit each other, to focus more directly on the needs of the investigation, and to verify each others' results.

In the new method, the investigator from the Sexual Crimes group will often postpone investigative actions, e.g., an interview with a suspect or a witness, in order to include questions or topics of interest from the digital investigator, or for results from a digital investigative step. Such results might be preliminary, but are in some cases useful as support in the interview or to confront the suspect.

The new method has also enabled the detection and investigation of larger-scale cases. Several recent cases have involved a large number of victims, while others have involved multiple offenders. In some instances the same victim or the same offender have been found in different cases, linking the cases together. We have been able to uncover the scale of these cases and their links because the digital investigators now have a more detailed understanding of the case and the people involved, and because the investigators at the Sexual Crimes Unit have a greater understanding of the possibilities and value of digital evidence.

In the old method, Sexual Crimes investigators would receive data extracted by the Digital Forensics Unit and use their regular work computers to investigate the data. These computers do not have the necessary computing power, network bandwidth, or software to conduct a forensic investigation. Now Sexual Crimes investigators have gained access to the computers, network, and some of the tools used by the Digital Forensics Unit. Digital investigators assist and train the Sexual Crimes investigators on how to correctly and efficiently use the tools. Both investigators now validate any findings. This means digital investigative steps are conducted more efficiently and in a more forensically sound manner.

Through the process of establishing this new method the Sexual Crimes Unit and the Digital Forensic Unit has visited international conferences and communicated with law enforcement agencies in the US, the UK, and the Netherlands. This exchange of knowledge and experience has influenced the process and the Sexual Crimes group reports that, in part because of this international influence, implementing the new method has helped shift the investigation from counting images and videos to focusing on victim identification.

In 2016, the National Criminal Investigation Service conducted a project to develop a national solution for handling abuse material. The establishment of the new method described here was a major driver to inaugurate this project, and it is a key component in the deliveries from the national project.

6. DISCUSSION AND CONCLUSIONS

We have reported on our preliminary findings from developing and fielding a new way of working crimes against children. Digital

and criminal investigators work closer together through all phases of the investigation. Results so far are positive.

Even so, criminal investigations and digital forensics must continually develop to address novel, criminal methods. We present a snapshot of the current practice at our law enforcement agency. Improvement is a continuous strive which includes developing best practice procedures, for example for conducting searches and handling of digital evidence in the field.

To further develop investigator cooperation we see the need for both groups to become more competent in each others' fields. Oslo Police District is conducting a pilot project on behalf of the Norwegian Justice Department as part of a national strategy to combat digital crime. A goal of this strategy is to increase the digital competence of the Norwegian police. The project will identify how the police can develop their capabilities to investigate and prevent digital crimes not handled by a national competence center. The method in this paper is employed as part of this project.

We have tried to qualitatively address a few questions in this paper, but in general many other research questions need to be quantitatively examined as well, both locally and in relation tointernational experience and circumstances. We are probably moving towards a world where 'one size fits all' will no longer work for digital forensics, if it ever did.

These are not only questions of technology and investigation, but also law, especially how the international, and changing, legal landscape affects digital investigations. Not all process developments are possible (or even desirable) to utilize world-wide. For example, deciding how much evidence is enough for conviction, as in the case of possessing child abuse material where the evidence may contain millions of images and videos. The question needs to be answered in relation to local law, interpretation and practise, even though we believe parts of the answer have more general applicability.

Acknowledgements

The authors would like to thank the members of the Digital Forensics and Sexual Crimes Units at Oslo Police District for their support in writing this paper. In particular we wish to thank Eline Liljedahl and Fredy Salazar, heads of the crimes against children groups at the Digital Forensics Unit and at the Sexual Crimes Unit, respectively, for comments that greatly improved the manuscript.

This research was supported in part by the Research Council of Norway (RCN), under grant (248094); the ArsForensica project.

REFERENCES

[1] I. Alawadhi, J. C. Read, A. Marrington, and V. N. L. Franqueira. Factors influencing digital forensic investigations: Empirical evaluation of 12 years of dubai police cases. *Journal of Digital Forensics, Security and Law*, 10(4):7–16, 2015.

[2] E. Casey. Triage in digital forensics. *Digital Investigation*, 10(2):85 – 86, 2013. Triage in Digital Forensics.

[3] E. Casey, G. Katz, and J. Lewthwaite. Honing digital forensic processes. *Digital Investigation*, 10(2):138 – 147, 2013. Triage in Digital Forensics.

[4] G. Gogolin. The digital crime tsunami. *Digital Investigation*, 7(1–2):3 – 8, 2010.

[5] A. Irons and H. S. Lallie. Digital forensics to intelligent forensics. *Future Internet*, 6(3):584, 7 2014. ISSN: 1999–5903.

[6] J. I. James. Multi-stakeholder case prioritization in digital investigations. *The Journal of Digital Forensics, Security and Law: JDFSL*, 9(2):59, 2014.

[7] National Criminal Investigation Service. Datakriminalitet. In Norwegian, https://www.politi.no/kripos/datakriminalitet/ visited 2017-03-23.

[8] Oslo Police District. Foreløpig rapport fra pilotprosjektet om ikt og internett i politiarbeidet. In Norwegian, January 2017.

