# ArsForensica Workshop Oslo (On-line)

# 1st and 2nd of December 2020

The Ars Forensica project invites you to attend our international digital workshop the 1st and 2nd of December 2020 . Ars Forensica focuses on computational forensics for large-scale fraud detection, crime investigation and prevention. The project is funded by the Research Council of Norway (RCN) within the IKTPLUSS -program.

The overall objective of Ars Forensica is to provide new knowledge that can significantly improve the prevention, preparedness, investigation and prosecution of incidents in ICT environments, without compromising privacy and the rule of law.

Ars Forensica addresses topics related to the following:

- ♦ Robust and secure (ICT) infrastructures and systems;
- ♦ Privacy-preserving technologies, and
- ♦ Interaction between technology, individuals and communities.

At this workshop you will get the latest news from our ongoing state-of-the research which includes presentations, demonstrations and discussions. The workshop will focus on 4 main areas:

1. IDS/Malware detection/analysis
2. Low level/storage
3. Social network/ransomware analysis/cryptocurrencies
4. Forensic quality assurance, Legal/regulatory aspects

NTNU CCIS

Center for Cyber and
Information Security

# Day 1: Tuesday the 1st of December

| Time | Content |
|---|---|
| **10:00 – 10:30** | **Welcome and Introduction to IDS/Malware detection/analysis**<br>Professor Katrin Franke |
| **10:30 - 10:55** | **Approximate search in intrusion detection and forensic data analysis**<br>Prof. Slobodan Petrovic |
|  | **Break (5 min)** |
| **11:00 – 11:30** | **Malware/attack analysis**<br>Dr. Andrii Shalaginov |
| **11:30 – 12:00** | **Dynamic analysis of binaries**<br>Sergi Banin, PhD candidate |
|  | **Lunch** |
| **13:00 – 13:10** | **Introduction to low level/storage**<br>Prof. Stefan Stefan Axelsson |
| **13:10 - 13:40** | **"In God we trust, all others bring data"**<br>Gunnar Alendal, Cand. Scient |
| **13:40 – 14:05** | **IoT evidence volatility**<br>Jens Petter Sandvik, PhD Candidate |
|  | **Break (5 min)** |
| **14:10 - 14:40** | **Efficient file carving or You still haven't found what you're looking for?**<br>Martin Karresand, PhD Candidate |
| **14:40 – 15:10** | **Metadata carving**<br>Rune Nordvik, PhD Candidate |
|  | **Summing up day 1**<br>Prof. Katrin Franke |

# Day 2: Wednesday the 2nd of December

| Time | Content |
|---|---|
| 10:15 – 10:30 | **The adversary's intent - What are they really after?"**<br>Dr. Geir Olav Dyrkolbotn |
| 10:30 - 10:55 | **Topic Modelling**<br>Kyle Porter, PhD Candidate |
| | **Break (5 min)** |
| 11:00 – 11:30 | **Dark web/fora communication patterns**<br>Jan William Johnsen, PhD Candidate |
| 11:30 – 12:00 | **Cryptocurrency forensics: tracing and deanonymization**<br>Dr. Mariusz Nowostawski |
| | **Lunch** |
| 13:00 – 13:10 | **Forensic quality assurance, Legal/regulatory aspects**<br>Prof. Katrin Franke |
| 13:15 - 13:40 | **Searching for gold: How Digital Forensics impacts Investigation Quality**<br>Stig Andersen PhD Candidate |
| 13:40 – 14:05 | **Technological Neutral Regulation in the Digital Forensics Process**<br>Jul Fredrik Kaltenborn, PhD candidate |
| | **Break (5 min)** |
| 14:10 - 14:40 | **Assessment of technology, transparency, etc.**<br>Radina Stoykova, PhD Canidate |
| 14:40 – 15:10 | **Comparison of Big Data Forensic Tools**<br>Merve Bas Seyyar, PhD candidate |
| | **Closing remarks**<br>Prof. Katrin Franke |

**On the next pages you will find further details of the program.**

# Day 1: Tuesday the 1st of December

## Prof. Slobodan Petrovic, PhD. Approximate search in intrusion detection and forensic data analysis

*Bio:* Slobodan Petrovic obtained his PhD degree from University of Belgrade, Serbia in 1994. He worked at Institute of Applied Mathematics and Electronics and Institute of Mathematics in Belgrade from 1986 to 2000. He also worked on various information security-related projects at Institute of Applied Physics, Madrid, Spain, from 2000 to 2004. Since 2004 he has been with Gjøvik University College and Norwegian University of Science and Technology (NTNU), where he teaches cryptology and intrusion detection. His research interests include cryptology, intrusion detection, and digital forensics.

*Abstract:* The presentation is about new constrained bit-parallel methods of approximate search in forensic data analysis and intrusion detection.

## Dr. Andrii Shalaginov, PhD. Malware/attack analysis

*Bio:* Andrii Shalaginov is a Postdoctoral Researcher in Digital Forensics at the Norwegian University of Science and Technology (NTNU) and holds PhD degree (2018) in Information Security from NTNU. His current research interest includes static and dynamic malware analysis, development of machine learning-aided intelligent computer viruses detection models and similarity-based categorization of cyberattacks in the Internet of Things ecosystem. Dr Shalaginov has been working as a security researcher for the UNICRI / EUIPO framework related to malware analysis on copyright-infringing websites. He is also representative from Norway in the COST Action CA17124 "DigForAsp - Digital forensics: evidence analysis via intelligent systems and practices". From before, Andrii holds MSc in Information Security at the Gjøvik University College and BSc / MSc degrees in System Designing from the Kyiv Polytechnic Institute. Besides, Dr Shalaginov has extensive industry experience in software engineering, including Samsung, and developed several malware analysis and machine learning open-source projects.

*Abstract:* Sophisticated malware attacks in recent years showed that it is not only personal computers or servers that can be affected, but also a wider range of portable and embedded devices. Once the attacks are successful, it will likely lead to dramatic impact on individual's lives and societies. To be able to mitigate this, there have been developed many computational intelligence models capable of learning from characteristics of malicious software and detecting even modified previously unseen samples. However, malware developers tend to invent new ways of evading Machine Learning that decrease efficiency of such models. As a response to this, new models incorporating high levels of abstraction through deep learning and new approaches to robust malware characteristics extraction have to be proposed. Development of robust novel intelligent malware detection models will allow security agencies to keep up with the overwhelming number of malware samples appearing each day. Finally, this will lead to more efficient utilization of human resources required to manually analyze each malware sample.

## Sergi Banin, PhD candidate Dynamic analysis of binaries

*Bio:* Sergii Banin is a PhD candidate in NTNU. He received Master degree in Information Security from NTNU in 2016 and Bachelors Degree in Computer Engineering from National Technical University of Ukraine “Kiev Polytechnic Institute” in 2014. His research interest includes malware analysis and detection as well as the use of Machine Learning algorithms in such tasks.

*Abstract:* I am about to show how memory access traces produced before the Entry Point can be used to detect novel (previously unseen) malware.

# Day 1: Tuesday the 1st of December

DAY 1

## Prof. Stefan Axelsson, PhD. Introduction to low level/storage

Bio: Stefan Axelsson is a professor of digital forensics and cyber security at Stockholm University and a visiting professor of digital forensics at NTNU. He was previously an associate professor at NTNU funded by the Norwegian Police University College and the Norwegian National Criminal Police. His research interests include detection of undesirable events (fraud, computer intrusions etc.) and the investigation of these events.

*Abstract:* I will introduce why low level analysis is useful in a scenario such as this, and what challenges an investigator might face.

## Gunnar Alendal, Cand. Scient "In God we trust, all others bring data"

*Bio:* Gunnar Alendal holds a cand.scient. degree in Cryptography from the University of Bergen, UiB, Norway. He specialize in the use (and abuse) of cryptography, reverse engineering, malware detection, security vulnerabilities and exploitation. He has worked for the less public parts of the Norwegian Armed Forces and more public companies like Anti-virus company Norman. In recent years he has been working mainly with digital forensics at NCIS Norway (Kripos).

*Abstract:* No data, no digital forensics. Mobile phones are one of the most valuable data sources in digital forensics. The mandatory security and encryption of modern devices prevent law enforcement from performing data acquisition. I will introduce the current challenges and present my research of how law enforcement can research and develop offensive techniques, using security vulnerabilities and exploitation, to bypass security and encryption.

## Jens Petter Sandvik, PhD Candidate IoT evidence volatility

*Bio:* Jens-Petter Sandvik is a PhD candidate in Digital Forensics in the Testimon Digital Forensics Lab at NTNU, where the focus is on new challenges for digital forensics introduced by Internet of Things (IoT) systems. Since 2006 he has also been working on digital forensics at the National Criminal Investigation Service (Kripos), first with mobile and embedded systems forensics, and later with cloud and network forensics, and cryptocurrency investigations.

*Abstract:* As the popularity of IoT systems is increasing, the systems will inevitably become part of both the crime scene, the tools for commiting crimes, and the target of crimes. In this talk I will go more in detail on one operating system for IoT devices, and look closer on the volatility of the data stored in these types of devices.

## Martin Karresand, PhD Candidate Efficient file carving or You still haven't found what you're looking for?

*Bio:* Martin Karresand is a Senior Scientist in IT security at the Swedish Defence Research Agency where he has worked since 2003. He got his Licentiate degree in Engineering at Linköping University, Sweden, and is currently a part time PhD candidate at NTNU. He has previously worked as a forensic engineer at the Swedish National Laboratory of Forensic Sciences (currently the Swedish National Forensic Centre). His research interests include file carving, forensic data mining, machine learning and all sides of technical computer security.

*Abstract:* When you lose your keys you search for them at the place where you lost them, not linearly all around the globe. In file carving the latter strategy is unfortunately used. My research aims to find the most probable logical position on disk of different types of data, which will greatly reduce the time used to find interesting data in storage media.

# Day 1: Tuesday the 1st of December

## Rune Nordvik, PhD Candidate, Metadata carving

*Bio:* Rune Nordvik is a Lecturer at the Norwegian Police University College at the Nordic Computer Forensic Investigator studies (NCFI) and a part time PhD candidate at the NTNU. He holds a Master in Information Security from NTNU Gjøvik (previously Gjøvik University College). He has worked as a digital forensic expert at the Nordmøre and Romsdal Police District. His research interests include file system metadata, carving techniques, validation of processes and verification of digital forensic tools.

*Abstract:* Digital forensics depends on automated tools in order to perform an efficient investigation. However, how do we know that the tools we depend on are accurate and include all relevant metadata? How can we trust the tool vendor when they are developing close source tools, protected by intellectual property rights, or treated as secrets, not peer-reviewed, not verified, and not validated properly by law enforcement? Data used in digital forensics are found in file systems, either located on the storage of a computer, a tablet, a mobile phone, a smart watch, an IoT-device, a Drone, an infotainment system in a car, in the storage of an electrical vehicle fast charger, on a cloud storage, etc. My research focuses on unknown or not understood metadata structures and assess their relevance for investigation purposes. In this talk I will focus on using near co-located timestamps as a dynamic signature in order to carve for inodes (metadata) in an Ext4 file system, and how this can help the investigation to recover more files from a damaged file system. Ext4 is important since it is often used by Android mobile devices, IoT devices, or Linux desktop or server systems. The approach is generic, and can be used for other file systems with near co-located timestamps.

# Day 2: Wednesday the 2nd of December

## Dr. Geir Olav Dyrkolbotn, PhD. The adversary's intent - What are they really after?"

*Bio:* Maj/Dr. Geir Olav Dyrkolbotn is an officer in the Norwegian Armed Forces and an associate professor at Center for Cyber and Information Security (CCIS) at the Norwegian University of Science and Technology (NTNU). He is currently head of the NTNU Malware Lab and the research group for cyber defence at CCIS. Geir Olav holds a PhD in information security from Gjøvik University College (HiG) and a MSc in computer science from the NTNU. His career includes more than 25 years in the Norwegian Armed Forces, where he holds the rank of Major. His career has focused on operation, maintenance and security in tactical communication systems and the last 15 years on defensive cyber operations, computer network defense and operational security. His research interest includes cyber defense, reverse engineering and malware analysis, side-channel attacks and machine learning.

*Abstract:* The adversary's intent – What are they really after? Investigating a digital crime scene has many similarities to investigating cyber-attacks. We can dig into technical detail and find clues about what has happened. Pieces of the puzzle can be mapped onto the Cyber Kill Chain, in an effort to explain what happened. However, we also need to address, why did it happen? What is the intent of the adversary? What were they really trying to do? Answering this can be supported by low level forensic analysis and the kill chain, but also requires a different perspective. Investigating what the adversary is talking about may help us. This kind of information may be available in the dark web and underground forums. How do we better find and use such information? This is the focus in the next section.

## Kyle Porter, PhD candidate - Topic Modelling

*Bio:* Kyle Porter is a PhD candidate and research fellow in the Testimon Digital Forensics Lab at the Norwegian University of Science and Technology. His primary research interest is to increase the efficiency and effectiveness of finding relevant textual data or evidence in digital investigations. The methods being investigated include developing string matching algorithms for literal text matches, or applications of machine learning for intelligent data exploration.

*Abstract:* In this talk we briefly cover topic models, and how they can be used in the context of an investigation. Much of the talk will be looking at topic models that were extracted from real dark net market discussion forums, and how we can even find keywords such as cryptocurrency wallets and hidden services addresses.

## Jan William Johnsen, PhD candidate Dark web/fora communication patterns

*Bio:* Jan William Johnsen is a PhD candidate in the NTNU Digital Forensics Group at the Norwegian University of Science and Technology (NTNU). His research interests include data- and computational-driven investigation to proactively stop cybercriminal actors. The methods being investigated include graph theory and the application of machine learning to understand the complex phenomena of identifying high-profile cybercriminals.

*Abstract:* Traditional criminal groups move their activities into the cyber domain, where they form underground forums which serve as marketplaces for illicit materials, products and services. Technically proficient and high-skilled actors drive the Crime as a Service business model by offering illicit goods to lower-skilled cybercriminals. Focusing law enforcement efforts and resources on proficient actors has the highest impact of disturbing their activities. Our research involves data-driven analysis and contributes to uncovering proficient cybercriminals. The methods we employ are network centrality measures and natural language processing to enhance our result to differentiate between high- and low-skilled actors. Our approach can exclude a big portion of low-skilled actors to make network algorithms faster and infer the roles for remaining actors using topic modelling.

# Day 2: Wednesday the 2nd of December

## Dr. Mariusz Nowostawski, PhD. Cryptocurrency forensics: tracing and deanonymization

Bio: Mariusz Nowostawski obtained his PhD in the area of artificial life and self-evolving systems in University of Otago, New Zealand. He has worked in the area of self-* computing, software engineering, cyber security, machine learning and financial services. He is specialising in cryptocurrency forensics and the application of blockchain technology in combination with privacy-preserving techniques and autonomic computing.

Abstract: The talk will explore some of the aspects related to cryptocurrency forensics and explore techniques used in tracing and de-anonymising financial flows. We will introduce the main arising challenges and methods that are currently used.

## Stig Andersen, PhD Candiate, Searching for gold: How Digital Forensics impacts Investigation Quality

Bio: Stig Andersen is a special investigator with Oslo Police District. He holds a Bachelor of Informatics from University of Oslo, a Master of Science in Security and Forensic Computing from Dublin City University and is currently working on a PhD in Information Security at NTNU. Stig has previous experience from both public and private sector, and has worked with both NATO, OECD and a wide range of Norwegian organisations. Prior to engaging with the world of academic research, Stig's job at the department of digital policing involved investigating murders, sexual abuse, financial and organised crime, as well as developing new methods and techniques for practical digital forensic work.

Abstract: Investigating digital evidence is necessary to solving crime and to uncover and understand events in cyberspace. Incidents involving computer systems - regardless of the complexity, variety and prevalence of such systems - must be scrutinized in order to return the system to a safe and secure state, and to avoid repeating incidents. The situation is similar when criminal incidents are investigated, however, the end goal is different. This talk will present a general process of investigation applicable to both types of investigation, discuss how digital forensics relates to the investigation process and how it impacts quality.

## Jul Fredrik Kaltenborn, PhD candidate, Technological Neutral Regulation in the Digital Forensics Process

Bio:Jul Fredrik Kaltenborn is a teacher at the Police University College in Stavern and a PhD- candidate at the faculty of law in Oslo (UiO). He holds a master degree (diplôme de commerce) from Ecôle de Management de Lyon and he is cand. jur. (lawyer) from the University of Oslo. Jul Fredrik has previous work experience from both France (private sector) and Norway (public sector). Relevant positions for his PhD-project are his position as a Deputy Judge in Stavanger District Court and his position as a Prosecutor in Økokrim.

Abstract: I will present technological neutral regulation in digital forensics and explain why a new concept of the term is needed. Finally, some of the requirements for the new concept will be pointed out.

# Day 2: Wednesday the 2nd of December

## Radina Stoykova, PhD Canidate, Assessment of technology, transparency, etc

*<u>Bio:</u>* Adi Stoykova holds a Master`s degree in law from Sofia University, "St. Kliment Ohridski", Bulgaria and LL.M. in IT and IP law from Leibniz University Hannover, Germany. Currently, she is working on a dual PhD between the University of Groningen (RUG) and the Norwegian University of Science and Technology (NTNU) as part of the ESSENTIAL project: https://www.essentialresearch.eu/. The topic of her PhD is “Standards for digital evidence” and it is focused on developing digital forensic procedures and practices to comply with forensic validation requirements and human rights standards.

*<u>Abstract:</u>* I will talk about the changes in digital forensics scope, methods, and tools introduced by IoT scenarios and data volumes and why this imposes challenges to the fair trial and to the reliability of the digital evidence as a result of the computations.

## Merve Bas Seyyar, PhD candidate - Comparison of Big Data Forensic Tools

*<u>Bio:</u>* Merve Bas Seyyar is a PhD candidate at the University of Groningen and the Norwegian University of Science and Technology as part of the ESSENTIAL (Evolving Security SciencE through Networked Technologies, Information policy And Law) Project. Her PhD research lies at the intersection of privacy, digital forensics and big data. Main objective of her PhD is to promote the discussion on how to detect and limit privacy exposures during digital investigations. She is currently working at the Netherlands Forensics Institute as a trainee.

*<u>Abstract:</u>* The presentation is about the comparative analysis of three big data forensics tools in terms of efficiency, capability, speed and usability.

Very welcome!!!