# THE IMPACT OF MOBILE NETWORK FORENSICS EVIDENCE ON THE CRIMINAL CASE PROCESSING PERFORMANCE IN MACEDONIA: AN INSTITUTIONAL ANALYSIS STUDY

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Filipo Sharevski

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

December 2015

Purdue University

West Lafayette, Indiana

This dissertation is gratefully dedicated to all the people who never stop believing in me.

# TABLE OF CONTENTS

Page

Page

Page

# LIST OF TABLES

Table Page

# LIST OF FIGURES

Figure Page

Figure Page

Figure Page

# LIST OF ABBREVIATIONS

2G/3G/4G/4G+ - Second/Third/Fourth/Beyond Forth Generation of Mobile Technology
3GPP - 3rd Generation Partnership Project
AuC/EIR - Authentication Center/Equipment Identity Register
BSC/BSS/ BTS - Base Station Controller/ Subsystem/Transceiver
CC - Content-of-communication
CDR - Charging Data Records
CEPEJ - European Commission for the Efficiency of Justice
CGI - Cell Global Identity
CID - Communication Identifier
DHCP - Domain Host Configuration Protocol
DNS - Domain Name System
EU - European Union
GDP - Gross Domestic Product
GERAN/UTRAN/E-UTRAN – GPRS/UMTS/Evolved Radio Access Network
GGSN - Gateway GPRS Support Node
GPRS - General Packer Radio System
GPS - Global Positioning System
GSM - Global System for Mobile
HLR - Home Location Register
HSPA/HSUPA/HSDPA - High Speed Packet Access/Upload/Download
IAD - Institutional Analysis and Development Framework
ICCID - International Circuit Card Identification
IMEI - International Mobile Equipment Identification
IMS - Internet Multimedia Subsystem
IMSI - International Mobile Subscriber Identification
IP - Internet Protocol
IRI - Intercept Related Information
ISO/IEC - International Standardization Organization/International Electrotechnical Commission
ISP - Internet Service Provider
ITU - International Telecommunication Union
LAC - Location Area Code
LAI/RAI - Location Area Identifier/Routing Area Identifier
LDI - Location Dependent Interception
LTE - Long Term Evolution
MCC - Mobile Country Code

ME/MT - Mobile Equipment/Mobile Termination
MNC - Mobile Network Code
MOC - Mobile Originating Call
MSC - Mobile Switching Center
MSIN - Mobile Subscription Identification Number
MSISDN - Mobile Station Integrated Services Digital Number
NDFL – National Digital Forensics Laboratory
NLEA – National Law Enforcement Agency
NIST - National Institute of Standards and Technology
PCRF/PCEF - Policy and Charging Rules Function/Enforcement Function
PIN - Personal Identification Number
PLMN/HPLMN/VPLMN - Public Land Mobile Network/Home/Visited
PUK - PIN Unlock Key
RNC - Radio Network Controller
SGSN - Serving GPRS Supporting Node
SIM - Subscriber Identification Module
SMS/MMS - Short Message /Multimedia Message Service
TDMA/FDMA - Time Division /Frequency Division Multiple Access
UMTS - Universal Mobile Telephone System
VLR - Visitor Location Register

# ABSTRACT

Sharevski, Filipo. Ph.D., Purdue University, December 2015. The Impact of Mobile Network Forensics Evidence on the Criminal Case Processing Performance in Macedonia: An Institutional Study. Major Professor: Melissa J. Dark.

The purpose of this study was to explore the contribution of the localization data, network-management data, and content-of-communication data in the case processing performance in Macedonia. The mobile network forensics evidence was analyzed respective to the impact of the mobile network data variety, the mobile network data volume, and the forensic processing on the case disposition time. The results from this study indicate that the case disposition time is negatively correlated with the network-management data volume and positively correlated with the content-of-communication data volume. The relevance of the network-management data was recognized in the highly granular service behavior profile developed using larger number of records, while the relevance of the content-of-communication data was recognized in the substantial number of excerpts of intercepted communication. The results also reveal a difference in the case processing time for the cases where there is only localization or network-management data versus when they are combined with the content-of-communication data.

# CHAPTER 1. INTRODUCTION

The processing of mobile-enabled crimes is increasingly burdened with voluminous and divergent mobile-related data pertaining to the criminal act. With 119.7 petabytes of mobile traffic generated per month, the timely process of justice is directly affected by the time consumed for the associated evidence handling (Cisco, 2015). This predicament is relevant for the Macedonian criminal justice system, which is already under-performing in the general allocation of criminal justice. Concentrated on the mobile-related judicial and forensics practice, this dissertation utilized the Institutional Analysis and Development (IAD) framework to explore the effect of the mobile network data on the case processing performance.

## 1.1. Statement of the Problem

As a consequence of the mobile service proliferation, the criminal justice system in Macedonia needs to increase its efficiency respective to the mobile-enabled crime processing (UNODC, 2013). The 109.1% active subscriptions and 71% of compound annual growth rate of mobile traffic can aggravate the *in-time* case processing and the *multi-jurisdictional collaboration* in that the mobile network evidence necessitates specific forensics preparedness that most judiciaries lack (Rajamaki & Knuuttila, 2013). Consequently, the main concern for the Macedonian criminal justice system is the proper juristic utilization of the mobile network data as a vehicle for performance improvement. To explore how the mobile network data affect the process of justice, the recent mobile-enabled crime processing in Macedonia is set at the focus of this study.

## 1.2. Research Question

The research question explored by this dissertation follows as:

Currently, how *localization* data, *network-management* data and *content-of-communication* data (3rd Generation Partnership Project, 2014d) affect the criminal case processing within the Macedonian criminal justice system?

## 1.3. Significance of the Problem

Mobile evidence is routinely involved in crime, given the 99% of mobile service global penetration and the 3 billion active smartphones (Ericcson, 2015). Accordingly, the emerging crime is “a critical challenge for the judiciaries in the developing countries, requiring comprehensive forensic support” (UNODC, 2013). In this context, Macedonian judiciary is in direct peril of institutional collapse if the mobile network data are not prioritized in the delivery of criminal justice (Helfenstein & Saariluoma, 2014). Therefore, the study analyzed the mobile network data effect on the criminal justice allocation performance for the mobile-enabled crimes. The findings are of immediate usefulness for the operative actions in response to the emerging mobile-enabled crime. They are relevant for the recognition of the mobile network data as a valuable juristic evidence as well as for an extended multi-jurisdictional collaboration. Given the critical role of the mobile technology, they are also useful for any criminal case processing that involves any of the mobile data types included.

## 1.4. Purpose of the Study

The purpose of this study was to explore how the mobile network data contribute to criminal case processing in Macedonia. The focus was set on the impact of the mobile network data variety, volume and forensics processing on the case processing performance. Of interest were the *content-of-communication data* or the conversation carried over the mobile network, the *localization data* or the geolocation trace of the parties involved in the crime as logged by the mobile network infrastructure, and the *network-management data* or the mobile service behavior of the parties involved. A convenience criminal case sample including these mobile data types was analyzed using the IAD framework in response to the research question. The framework was particularly chosen to capture the overall effect of the mobile network data in a juristic context, that is, to understand the relevance and the perception of the mobile technology within the institutional settings of the Macedonian criminal justice system.

## 1.5.Assumptions

The assumptions relevant to this research study were:

1. The convenience sample of mobile-enabled cases provided the most informative insight into the associated case processing practice of the Macedonian criminal justice system as of the period this study was executed.
2. This study assumed normality of all data and used parametric statistics.
3. The mobile network data used as evidence possess no threats to the privacy of the entities related to nor to the integrity of the Macedonian criminal justice system. It

was assumed that all anonymization measures have already been taken by the prosecution.

4. The use of the 3rd Generation Partnership Project and International Standardization Organization SC27 standards are valid means of worldwide mobile and digital forensics standardization, respectively.
5. The European Commission for the Efficiency of Justice (CEPEJ) performance evaluation provided an accurate EU judiciary profile and criteria for judicial performance assessment for the period this study was executed.

## 1.6. Limitations

The limitations relevant to this research study were:

1. The classified access to the case reports, the extensive case data volume, and the unstructured case logs imposed selection of cases with a moderate amounts of mobile network data included as an evidence. The reason was to provide enough time for collection, codification and subsequent analysis of the case data. This limits the generalizability of the research findings only to the part of the mobile-enabled cases population that involve a moderate amount of mobile network evidence.
2. The convenience selection accented the local jurisdiction in all the possible mobile-enabling contexts. One cross-territorial (or multi-jurisdictional) case was included to account for the context where network-management evidence might be retrieved from other jurisdictions. Thus, the observations are not generalizable to cross-territorial cases that include localization or content-of-communication data due to the legislative limitations in retrieving this kind of evidence from other jurisdictions.

3. Because the sample in this study was not large enough to test for normality of distribution, the findings could be influenced by the use of parametric statistical methods.
4. The sample captures only the contribution of the mobile network evidence on the case processing performance of the mobile-enabled instances. There might be another types of digital evidence included in the sample population, but the findings do not extrapolate nor transfer to their contribution in the case processing performance.
5. The sample captures the contribution of the mobile network from two aspects: variety and volume, and forensic processing. That is, the variety refers to the number of mobile network data types included in a given case while the volume refers to the number of records or hours of conversations. It does not directly refer to the number of target identities or the investigation period for which these records/hours were collected. The forensic processing effect refers to the probative aspect of the mobile network data, that is, its relevance as a juristic evidence.
6. The contribution of the mobile network evidence was explored as of its expedious effect on the case processing performance. There might be other mobile-enabled crimes where the evidence has different effect, but the findings cannot be generalized to those type of criminal cases or in reference to those effects.
7. The localization data, network-management data, and the content-of-communication data are considered as of the third generation of mobile networks (3GPP). The same data types might refer to similar categories of mobile network information in the subsequent generations of mobile technology as the fourth generation (4G) Long Term Evolution or the 4G+ Long Term Evolution Advanced, but the results cannot be

generalized or transferred to crimes involving evidence from these mobile infrastructures.

8. Because the convenience sample has only seven cases, the findings may not be generalized to the entire space of mobile-enabled crimes. This limits the extrapolation of the conclusions only to the crimes that involve *localization*, *network-management*, and *content-of-communication* data types. That is, there might be other ways in which the mobile technology can facilitate a criminal activity, but the conclusions does not refer to those crime types.
9. The broader reliability of this study was demonstrated on the account of the operationalization of the research variables and the analytical instrument. The consistency of the operationalization procedures with the 3GPP, ISO SC27, and the CEPEJ guidelines ensures replicability of the findings when these guidelines are used to study mobile network data in the context of juristic evidence. The IAD framework ensures that the inquiry is consistent with the institutional structure of any criminal justice system and it can be replicated in terms of the relationship between the forensic and juristic processing of mobile network evidence. However, the variations in juristic decision making, the differences in the evidence perception in relation with other evidence, and the potential changes in the institutional attributes of the Macedonian criminal justice system over time prevented establishing reliability in the traditional sense for this study.

## 1.7. Delimitations

The delimitations relevant to this research study were:

1. The European Commission of the Efficiency of Justice have developed two case processing performance indicators, the case disposition time and the clearance rate. This study used only the case disposition time as the response variable, given that it assesses the criminal performance within a criminal case log. The clearance rate assesses the performance between different criminal case logs, falling out of scope of this study. The IAD analysis was placed on the operational and collective-choice levels of institutional abstraction. The constitutional level analysis refers to the general crime processing, falling out of scope for this research study.
2. The Institutional Analysis and Development (IAD) framework in this study was used to *explore* rather than to predict the outcomes of the mobile-enabled crime processing in Macedonia.
3. The mobile network evidence considered in this study covers any electronically stored or transmitted data on or over a third generation (3GPP) mobile network infrastructure directly related to the control or user traffic. Any other evidentiary data associated with any previous or future generations of mobile network communication is excluded from this study.
4. The mobile network technology standardization, digital forensic specifications, judicial performance appraisals, and the mobile-enabled crime studies relevant for this research study were the ones available in 2015. That is, the study was delimited by the 3GPP technical specifications for the mobile network technology, the ISO

specifications for forensic management of the mobile data, and by the European Commission for the Efficiency of Justice for the case disposition effectiveness.

## 1.8. Definitions of Key Terms

3rd Generation Partnership Project (3rd Generation Partnership Project, 2014e, p. 1):

3GPP is officially recognized global standardization organization established to prepare, approve and maintain globally applicable Technical Specifications and Technical Reports for an evolved 3rd , 4th, 4th+ and beyond mobile networks.

3rd generation of mobile networks (3rd Generation Partnership Project, 2014e, p. 2):

Mobile network capabilities originally evolved from the Global System for Mobile (or the 2nd generation). These capabilities include mobility management, global roaming, utilization of relevant Internet Protocols, improved security, as well as increased download and upload speeds in the radio access network.

4th / 4th generation of mobile networks (3rd Generation Partnership Project, 2014e, p. 2)

Mobile network capabilities evolved (or planned to evolve in the future) from the 3rd generation of mobile communication onwards. Designated as the Long Term Evolution or the LTE standard (LTE Advanced for the 4th+ generation) they include interoperability cloud computing platforms, high-definition mobile TV, augmented web services, and increased data rates in the radio segment.

Content-of-Communication (3rd Generation Partnership Project, 2014e, p. 16):

Information exchanged between two or more users of a 3G mobile network service in both real and non-real time and excluding intercept related information.

Forensics processing of mobile-enabled crimes (Palmer, 2001):

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and reporting of digital evidence derived from mobile network infrastructure for the purpose of facilitating or furthering the reconstruction of criminal events. Respectively, the effort invested for the forensic processing is measured as the time spent on these phases comprising the mobile network evidence production.

Juristic processing of mobile-enabled crimes (CEPEJ, 2014)

> The delivery of criminal justice is governed by the legislative framework, involving case administration and investigation led by the prosecution and courtroom case resolution led by ruling judges, including the mobile network evidence in the formulation and testing of the criminal hypothesis developed for the associated case. The effort and time encompassing the respective actions is assessed as the case processing performance and aggregates the effort and time spent for forensic processing of the mobile network evidence used for the purpose of facilitating or furthering the reconstruction of criminal events.

Localization Data (3rd Generation Partnership Project, 2014e, p. 6):

> Information associated with 3G mobile network services involving users' movement pattern, mainly referring to the localization data used for user positioning for a subsequent service delivery.

Mobile-enabled Crime (ITU Cybersecurity Division, 2009; Perry & Carter, 2011):

> Any crime or violations of criminal law facilitated or committed using a 3G mobile service, involving knowledge of mobile technology for their perpetration.

Mobile Network Evidence (International Standardization Organization, 2014b, p. 2):

Information/data stored or transmitted by the mobile network that may be relied on as evidence, using to support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi; It is a superset of three different data types: content-of-communication data, network-management data, and localization data.

Mobile Network Operator (3rd Generation Partnership Project, 2013, p. 23):

The entity which offers telecommunications services over an air interface and have an operational, 3GPP compliant mobile network from the third generation.

Network-management Data (3rd Generation Partnership Project, 2014e, p. 6):

Information associated with 3G mobile network services involving users' service behavior, mainly referring to the infrastructural data used for service realization.

Target Identity (3rd Generation Partnership Project, 2014d):

A technical identity that uniquely identifies a target of interception. One target may have one or several network IDs: MSISDNs, IMEI, or IMSI number (p. 6).

## 1.9. Summary

This chapter presented the goal of the study, the research question, the scope and the significance of the research problem, and the purpose of the research inquiry. The assumptions, limitations, and delimitations framing the outcome of the study were also described within. The next chapter presents the background of this study, bringing the relevant details on the Macedonian criminal justice system and the mobile-enabled crime processing. The literature review extends on its juristic performance, the structure of the mobile network evidence, and the instrument for the institutional analysis..

# CHAPTER 2. LITERATURE REVIEW

This chapter inspected the case processing function of the Macedonian criminal justice system with an accent to the mobile-enabled crime segment. Using the IAD framework, the structure of the Macedonian judiciary was decomposed respective to the present biophysical conditions, community attributes, and rules-in-use. The practice in combating emerging crime was included to emphasize the significance of the research problem and the purpose of the study. A separate section was dedicated for the nature of the mobile network data and the institutional context of the study in general.

## 2.1.The Anatomy of the Macedonian Criminal Justice System

### 2.1.1. Physical and Material Characteristics

#### 2.1.1.1.Case Processing Function – Provision and Production

Mobile-enabled crimes are processed relative to their jurisdictional provenance, the data type(s) needed and the crime hypothesis developed for a given case. For local crimes where localization and/or network-management data are needed, the evidence is yielded in coordination with the operators and the National Digital Forensics Laboratory (NDFL). For local crimes where content-of-communication data are needed, the evidence is acquired and delivered by the National Law Enforcement Agency (NLEA) in real-time. In all cases, the mobile network evidence production follows a previously communicated crime hypothesis including the *target identities* and the *investigation timespan* for which the mobile network data. The retrieval of cross-territorial evidence is realized over the Ministry of Justice responsible liaisons (Assembly of the Republic of Macedonia, 2008a; The Council of the European Union, 2001). Once the mobile network data is in forensic custody, the NDFL processes it according to the criminal hypothesis to produce the mobile network evidence, which is returned to juristic custody and subsequently presented in Court.

#### 2.1.1.2.Financial Resources for Judicial Provision and Production

The Macedonian judiciary receives far lower budgetary support of €0.55 billion compared with the EU average of €400 billion per year. The budget accounts 82.5% for salaries (70% EU average), 0.4% for computerization (3.1% EU average), 3.8% for training (11.7% EU average) and 13.3% in other expenses (CEPEJ, 2014).

#### 2.1.1.3.Human Resources for Judicial Provision and Production

There are 688 professional judges at disposal (697 EU average) that receive annual remuneration of €17,252 (€47,789 EU average). The compensation is -12.1% of the national average gross salary, suggesting slight diminishment in the appreciation of their societal role. On a yearly basis, judges receive a "general in-service training for specialized functions, recent trends in emerging crime, and cross-European computer crime processing" (The European Commission for the Efficiency of Justice, 2013).

There are 207 prosecutors covering the national jurisdiction (209 EU average). Maintaining equal balance between the prosecutors and judges, the salaries and the training received are equally endowed for both gilts. Relative to the experts support, Macedonian judiciary has 103.3 experts per 100,000 inhabitants, beyond the EU average of 67.6. However, there is no information on the number of designated mobile-enabled crime processing experts.

#### 2.1.1.4.Technologies Relevant for Mobile-Enabled Crime Processing

A digital forensics laboratory and an interception infrastructure are necessary in producing the mobile network evidence. The National Digital Forensics Laboratory (NDFL) was established at the beginning of 2013 and equipped with the relevant hardware and software solutions. However, it is still not accredited according to the ISO/IEC 17025 standard for competence and conformity of forensic laboratories (International Standardization Organization, 2005). There is no proof that the laboratory possesses any specialized software solution for examination, analysis and interpretation of mobile network data. The forensic practitioners have received training on the "approaches for the forensic examination and use of digital evidence for juristic purposes" (European Network of Forensic Science Institutes, 2009). The National Law Enforcement Agency (NLEA) has established a basic interception infrastructure with all the mobile networks operating in Macedonia (3rd Generation Partnership Project, 2014d, 2014e). Due to the sensitivity of the deployment details, no information is publically disclosed as of the 3GPP compliance and the procedures employed for traffic interception.

#### 2.1.1.5.Storage Requirements and Distribution Channels

The mobile network evidence as *big* data (Quick & Choo, 2014) entails separate storage facilities and distribution channels. The Macedonian criminal justice system is supported by a encryption-protected IP backbone infrastructure with "13 large-scale cloud storage servers and 100 working stations" (Ministry of Justice of the Republic of Macedonia, 2007, p. 23). There are three evidence distribution channels. The first one is with the Ministry of Interior Affairs and enables secured and confidential distribution of the intercepted material from the local mobile network operators. The second one is towards each of the mobile operators, enabling delivery of retained mobile data needed as evidence. The last one is towards the Ministry of Justice and is designated for cross-territorial evidentiary retrieval (Assembly of the Republic of Macedonia, 2008a).

#### 2.1.1.6.Scale and Scope of the Criminal Case Processing Function

The criminal caseload – scoped as per the Criminal Code of Macedonia – scales as a one tenth of the EU case volume. There are 14,694 versus 157,544 incoming cases, and 15,496 versus 152,113 outgoing cases in the last period of assessment (CEPEJ, 2014, p. 219). The scoping and scaling is assessed only to the criminal type, leaving no quantitative details on the technology enablers of the crime. However, considering the mobile communication reliance, the aforementioned scaling and scoping is relevant for the mobile-enabled crime processing in Macedonia (Ericcson, 2015).

### 2.1.2. Judicial Community Attributes

#### 2.1.2.1.Community Size and Structure

Next to the prosecutors, judges, mobile operators, NDFL, NLEA and the Ministry of Justice liaisons, the criminal case processing community involves also the Academy of Judges and Prosecutors. The Academy is relevant because it conducts the cybercrime training needed for the operational processing of the emerging crime. The curriculum includes modules on the cybercrime legislation, computer and internet architectures, jurisdictional competencies, the basics of electronic evidence, and investigative measures. However, there is no information on dedicated modules in respect the mobile network data and the associated crime processing.

2.1.2.2.Members' Values, Preferences, and Beliefs

The common institutional belief on the optimal allocative output rests on economic arguments. The modern judicial reform "changes the composition and characteristics of the factors of production and the production process to augment the quality of the output" (Hammergren, 2011). Therefore, there are regular cybercrime trainings, computer-related processing guidelines (Zvrlevski, Andonova, & Miloshevski, 2014), and the Ministry of Justice invested in a modern ICT infrastructure.

However, this reasoning does not bring straightforward results as anticipated by the European Commission for the Efficiency of Justice (2013). Obviously, the economic logic alone is not sufficient in improving the quality of justice (Dubois, Schurrer, & Velicogna, 2013). This extends towards the role the juristic self-governance plays in the efficient combat of the emerging crime. The self-governance ensures judicial *independence* and by that, distinguishes the judiciary from the other public services (Besley & Ghatak, 2006). The perception of independence enables judges to conform to the practice regulation while maintaining discretion in their decision-making (Salzberger, 1993). However, the resoluteness for "public services performance improvement meets a resistance within the judicial community" (Hammergren, 2011). The preferences in opposing the diminishment of the judicial power on behalf of the practice appraisals have negative repercussions on the innovations targeting performance improvement. In the case of mobile-enable processing this leads to a subjective valuation of the mobile network data as juristic evidence. Challenged to provide target number of resolved cases, judicial actors may not capitalize the probative value of the mobile network evidence available in the operative case processing. Notwithstanding this tension, the common belief is that the mobile network data is indeed catalytic to allocation of justice to the extent where the remaining juristic factors are conductive for an expedious case processing. Thus, it is reasonable to expect a common agreement in improving the case processing performance by using the mobile network data as a reliable evidence.

### 2.1.3. Juristic Rules-in-Use

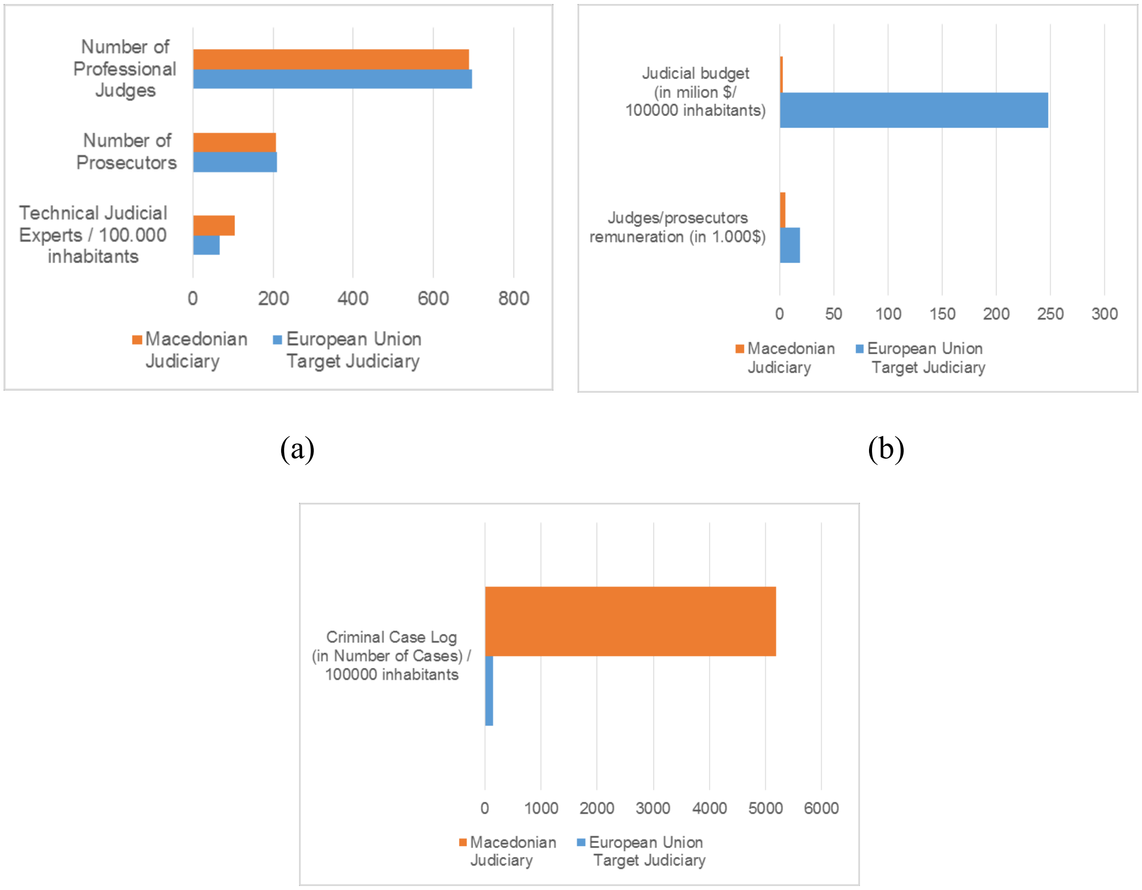
The rules-in-use correspond to actors' position, actions, and control, the information available, and the outcomes of the proceedings. The *boundary* rules align with the constitutional clauses §4 - §422 that define the criminal activity and the respective sanctions (Assembly of the Republic of Macedonia, 1991). The *position* rules align with the constitutional clauses §68, §98 and §102 and regulate judges' roles as triers-of-fact. The *Prosecution Act* defines the criminal process administration, while the *Code of Practice for Forensic Science* regulates the forensics involvement. (Assembly of the Republic of Macedonia, 1991, 2008b, 2010). As of the case processing actions and control, the *Criminal Code* and *Criminal Procedure Code* outline the *authoritative* and *scope* rules, respectively (Assembly of the Republic of Macedonia, 2013; Ministry of Justice of the Republic of Macedonia, 2005).

The *aggregate* and *information* rules define the legal syllogism employed in the criminal case processing. As such, judges evaluate the admissibility of the digital evidence according to its relevance, authenticity, being not a hearsay and unduly prejudicial, and being the best evidence. In this context, Sections B and D from the Criminal Procedure Code outline the mobile-enabled crime processing details. The previous details the role of the mobile network operators in acquisition and delivery of the retained evidence data whereas the live interception is given in the Telecommunication Interception Law. This law regulates the conditions under which the interception is a necessary measure, the interception procedures, and the storage, access and analysis of the intercepted material.

### 2.1.4. Summary – Macedonian Criminal Justice Profile

The *capacity for criminal justice delivery* of the Macedonian Judiciary and the target EU judiciary is contrasted in Figure 1. As of the human capital, Figure 1(a) suggests relative equivalence in the number of judges, prosecutors and technical experts available. In financial terms, there is a huge disproportion between the judicial budgets and judges' remuneration, according to Figure 1(b). Macedonian judicial budget is only 1.375% of its European counterpart, where the judges are receiving 64% more financial compensation then their peers. As of the workload, Figure 1(c) indicates a 97% larger case log than the European case log per 100.000 inhabitants. Macedonian administrators of justices need to process four times more criminal cases than their European colleagues, for which they receive a six-time smaller remuneration. Also, they have only a 1% of the financial resources for the criminal case processing at their disposal compared to the average judicial budget across the EU. In the mobile-enabling context (Ericcson, 2015;

UNODC, 2013), this comparison estimates the capacity available in delivering justice for the mobile-enabled crimes segment.



(a) (b)

(c)

*Figure* 1. Comparison between the Macedonian criminal justice system and the average for the European Union (target profile). (a) Human capital; (b) Financial support; (c) Workload.

## 2.2.The Performance of the Macedonian Criminal Justice System

The *case disposition time* is the key indicator of the case processing performance, developed and used by the European Commission for the Efficiency of Justice and it determines the number of days necessary for a pending case to be solved in court. Macedonian criminal justice system ranks 11st out of 17 criminal justice systems assesed by the European Commission for the Efficiency of Justice with a case disposition time of 211 days on average (Malta has 490, Italy 386, Slovenia 339, Spain 330,  Turkey 288, and Portugal 283 days of case disposition time). Twenty one judiciaries have not provided numbers on their average case disposition time. The risk of collapse is a plausible for the Macedonian criminal justice system considering the assessed 11.43% of lower efficiency than the average in case processing performance. To justify the significance of this study, the following section elaborates on the repercussions associated with the rapid growth in mobile-related criminal activities.

## 2.3. Mobile-enabled Crime and Criminal Justice Systems

A critical concern regarding the mobile-enabled crimes is to remain abreast of how the mobile technology is conducive to criminal activities (Brenner, 2012). The mobile evolution "translates into an inflation of devices ownership, allowing with a plausible opportunity to cultivate them in a sophisticated organization of the criminal activities" (Helfenstein & Saariluoma, 2014). From a criminal justice perspective, this trend challenges the juristic functioning because "it yields voluminous evidence that can spread across multiple jurisdictions" (Calderoni, 2010).

### 2.3.1. Juristic Management of Mobile-enabled Crime

The judicial response against the emerging crime trends is summarized by the UN Commission on Crime Prevention and Criminal Justice (2013). In regards the "judicial capacity to handle electronic evidence," almost all the judiciaries experience difficulties with the operative processing of the emerging crimes. The evidentiary data comes in large volumes and overburdens the forensic analysis. Accordingly, "more than 85% of the judiciaries have the electronic evidence admissible, with multiple means of presentation, and basic treatment as physical evidence"(UNODC, 2013, p. 165-168). Therefore, the production and application of electronic evidence remains a predicament in court.

UNODC (2013) has also extrapolated the findings with the recent ICT indicators as to indicate the emerging crime trend (Cisco, 2015; Ericcson, 2015). This is seen as a critical challenge for the judiciaries in the developing countries, requiring long-term, sustainable, and comprehensive technical and institutional support" (UNODC, 2013). On the technical side, the International Standardization Organization (2012) already took action to "harmonize the forensic methodology as to ensure legal admissibility of the digital evidence". A brief description on the SC27 family of standards is provided in understanding the mobile-related forensic processing.

### 2.3.2. Forensic Management of Mobile-enabled Crime

The International Standardization Organization (2012) devised international digital forensics accreditation through the set of interrelated documents depicted in Figure 2. The production of credible digital evidence begins by establishing investigative *readiness*, discussed within the ISO/IEC 27035:2011 *Information Security Incident Management* standard. The readiness phase encompasses: (1) *preparation for*; (2) *establishing capabilities for incident assessment*; (3) *respond to incidents* and (4) *post-investigation evaluation*. ISO/IEC 27035:2011 prescribes the common diagnosis strategies, and actions in real and non-real time response to cyber-related crime.

Presuming an ISO/IEC 27035:2011 readiness, the investigation follows the ISO/IEC 27037:2012 *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (International Standardization Organization, 2012). ISO/IEC 27037:2012 defines the *identification* as the "search for, recognition and documentation of potential digital evidence", followed by a *collection* and/or *acquisition* phase as to "bring the potential digital evidence under a forensics custody". Once the potential evidence is retrieved, the *preservation* takes place as to "protect its integrity as to ensure its usefulness for the investigation" (International Standardization Organization, 2012, p. 10). ISO/IEC 27037:2012 also defines the key investigation components as the chain-of-custody, crime scene responsibilities, and the core skills and competencies.

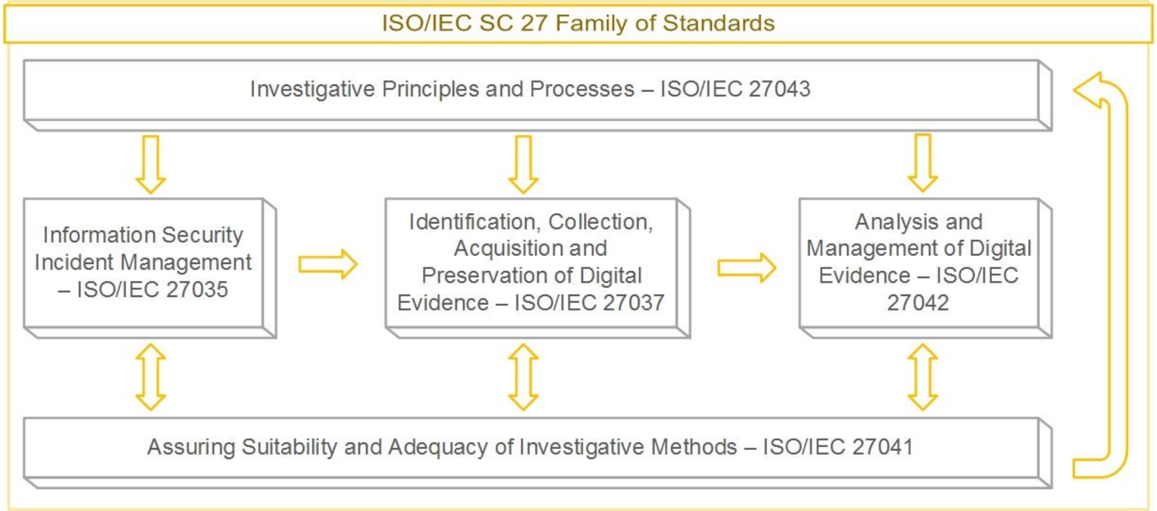

ISO/IEC SC 27 Family of Standards
Investigative Principles and Processes – ISO/IEC 27043
Information Security Incident Management – ISO/IEC 27035
Identification, Collection, Acquisition and Preservation of Digital Evidence – ISO/IEC 27037
Analysis and Management of Digital Evidence – ISO/IEC 27042
Assuring Suitability and Adequacy of Investigative Methods – ISO/IEC 27041

*Figure* 2. ISO/IEC SC27 Standards. Source: Adapted from (Marshall, 2011, p. 143).

ISO/IEC 27042 *Analysis and Management of Digital Evidence* brings the methodology for extracting the probative value out of the potential digital evidence. It includes iterative *interpretation* "to evaluate the evidence based on its contents and context including key patterns, topics, relevant people, etc. as to derive meaning" (International Standardization Organization, 2014a). This phase involves fact finding, impact analysis, validation/verification of results, and requires evaluation of the *likelihood-ratio* relative to the level of interpretative confidence. The ISO/IEC 27041 *Assuring Suitability and Adequacy of Incident Investigative Method* is provided as a guidance for assuring suitability and adequacy of investigative methods. This includes verification and confirmation directives assuring that the deliverable out of the digital forensic investigation is of utmost relevance for the criminal case processing.

ISO/IEC 27043 *Incident Investigation Principles and Processes* describes a *harmonized digital investigation schema*, "as a common investigation instrument across various operational scenarios involving digital evidence" (International Standardization Organization, 2014d). ISO/IEC 27403 outlines five classes of *investigative* proceess: readiness, initialization, acquisitive, interpretative and concurrent processes. In parallel, there is a set of *concurrent* actions: authorization, documentation, information flow management, chain of custody, digital evidence preservation, and interaction with the physical crime scene. The benefits of the model are: "human error minimization, balance between the investigative time constraints, costs, and evidentiary weight, and cross-border cooperation" (International Standardization Organization, 2014d).

In the research context, SC27 documents are a valuable reference that were used to understand the mobile network evidence production process, that is, to:

- Check whether an ISO/IEC 27035 readiness exists in practice;
- Learn whether the ISO/IEC 27037 guidelines are followed in the identification, collection, acquisition, and preservation of the mobile network evidence;

- Learn whether the ISO/IEC 27042 guidelines are followed in the analysis and management of the mobile network evidence in forensic custody;
- Find out which investigative principles, processes and methods (ISO/IEC 27041 and 27043) are implemented and which are not.

## 2.4.Mobile-enabled Crime – Technical Perspective

### 2.4.1. Digital Forensics Investigation in Mobile Networking Environments

Clark and Gibbs (2001) and Willassen (2003) intially discussed the forensic relevance of the mobile network data, focusing on the interception-related data and non-real time investigation basics. Forte and Donno (2010) recapitulate these concepts, providing the analytical aspects of the mobile interception and network-management data acquisition (3rd Generation Partnership Project, 2014e). In regards to localization evidence, Forte and Donno (2010) ordered the technical alternatives according to their accuracy and describe their practical utilization in an example investigation. Summa summarum, these works recap the recently technical perspective on the mobile-enabled crime. On the legislative side, Forte and Donno (2010) discuss the European Directives on “mobile traffic retention for the purposes of serious crime processing” (The Council of the European Union, 2006). Together with the legal interpretations of the cell tracking evidence (Blank, 2011; Herbert, 2014), and its admissibility (O’Malley, 2011), there exists no other literature reference. To gain the necessary forensics context of the mobile network evidence, the following section describes the mobile technology concepts.

### 2.4.2. Mobile Network Architectonics

Every mobile network deployment consists of two large logical segments, Radio and Core Network Subsystem, depicted in Figure 3 and Figure 4, respectively. The Radio Network Subsystem is divided in GSM/GPRS Radio Access Network (GERAN) and UMTS (UTRAN) parts enabling backward compatible access for all generations of mobile communication (Cox, 2014). The coverage area is logically divided in cells and sectors as to optimize the spatial distribution on the traffic. A unique Base Transceiver Station (BTS)/NodeB is associated with each cell, enabling basic user location management. The coverage scheme organizes all cells from a bigger geographical region into *Location Areas*, controlled by one or several Base Station Controllers (BSC)/Radio Network Controllers (RNCs). The BSCs and RNCs further interface towards the Core Network Subsystem as to enable full realization of the mobile services.

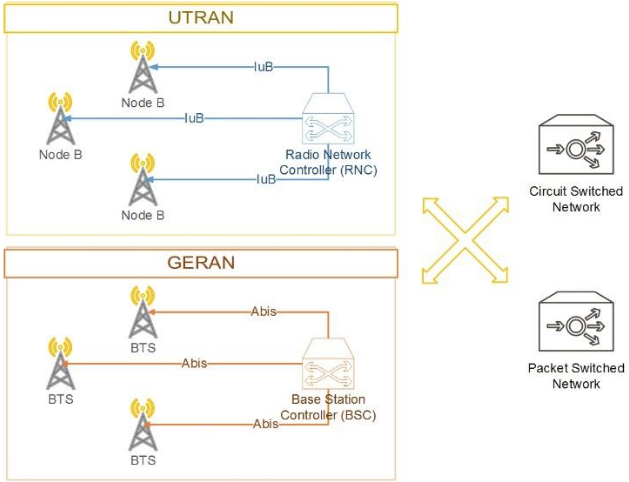


*Figure* 3. Radio Network Subsystem. Source: Adapted from (3rd Generation Partnership Project, 2002, 2008, 2014d).

Based on the service handling approach, there are Circuit and Packet Switched Networks. The Mobile Switching Centers (MSC) are the crux of the Circuit Switched Network because they control the call establishment, switching, interconnection and produce the Charging Data Records (CDRs or the network-management records). Alongside with the MSCs, the Home Location Register (HLR), Authentication Center (AuC), and Equipment Identity Register (EIR) perform the rest of the network-management logic. The Packed Switched network and the IP Multimedia Subsystem (IMS) are responsible for control and management of the packet services. The packet routing and user management functions are performed by the Serving GPRS Supporting Node (SGSN) and the Gateway GPRS Supporting Node (GGSN). The Policy Charging Rules/Enforcement Functions (PCRF/PCEF) are introduced in the third generation (3rd Generation Partnership Project, 2014c) and perform the charging function. Similar in the logical structure as the traditional internet service providers, the packet core and IMS enable mobile IP connectivity and concurrent service delivery.

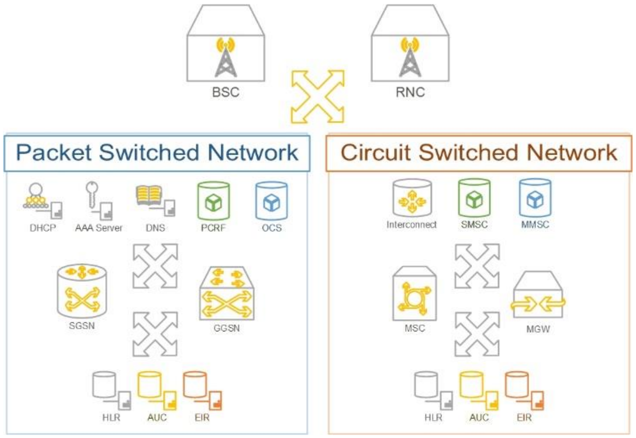


*Figure* 4.Core Network Subsystem - Circuit and Packet Switched Domains. Source: Adapted from (3rd Generation Partnership Project, 2002, 2008, 2014d).

### 2.4.3. Mobile Network Evidence

#### 2.4.3.1.Mobile Device Evidence Dependences

The target identity for the network investigation is extracted by a *mobile device* evidence retrieval. The practice of mobile device forensics encompasses extraction of the Subscriber Identification Module (SIM) data and the data on the mobile device itself (3rd Generation Partnership Project, 2007, 2012; Ayers, Brothers, & Jansen, 2014). The SIM or Universal SIM card has two globally unique identifiers: (1) Integrated Circuit Card Identifier (ICCID) distinguishing it among the smart cards; and (2) International Mobile Subscriber Identity (IMSI)[1], associating with a given mobile network at a time. Every equipment associated with the SIM card is uniquely identified by a vendor-specific International Mobile Equipment Identity (IMEI) number, managed by the EIR node. Mobile devices can provide information about the internal time settings, logs, contacts, and GPS related data, (Ayers et al., 2014; Glisson, Storer, & Buchanan-Wollaston, 2013).

#### 2.4.3.2. Network-management data

The network-management data valid as juristic evidence include:

**Mobile user identification set.** Includes the following set of identifiers: ICCID, IMSI, MSISDN, IMEI and the encryption keys (3rd Generation Partnership Project, 2014a).

**Charging Data Records.** Operators can provide information on the user service activity, registered in the so-called CDR or network-management records. The format of the CDR

[1] IMSI composition: first three - Mobile Country Code (MCC), next three - Mobile Network Code (MNC), and the rest nine form the mobile subscription identification number (MSIN).

of each different service, including the calling/called party, and duration of the call/session is given in (3rd Generation Partnership Project, 2014b).

### 2.4.3.3.Localization data

**Static Localization Evidence.** The historical movement pattern can be established using the following set of retained data (including the longitude and latitude of the position of the target identity at a given time) on the mobile network side:

- **Cell Global ID (CGI) –** Each registered user to the mobile network is uniquely associated with the Cell Global ID where he/she resides in a given point of time. This information enables creation of movement patterns and service activity maps for one or group of users. The CGI includes MCC, MNC, LAC and is unique within a given location area (3rd Generation Partnership Project, 2014a, p. 24)
- **Location Update Request –** each time the user is registered on the network or changes the residing cell/LAI (RAI), the location update procedure is invoked. The device reports its current cell, current VLRID/SGSNID and the network parameters according to which the initial geographical location can be determined (home or visiting network) (3rd Generation Partnership Project, 2015b).

**Dynamic Localization Evidence** – Another localization feature of forensics value is the *positioning* of the device associated with the user within network boundaries. Current 3G/LTE network deployments can approximately yield the position of a given user by the following mechanisms in real or near real time, ordered from least to most accurate:

- **Cell Identification –** triangulation of the geospatial cells/sector configuration with the timing advance. The accuracy is 200 m in urban 1 km in rural areas.

- **Observed Time Difference of Arrival –** device location can be tri-laterated i.e., calculated using the time difference of the arrival of the signal from each (e)NodeB. The accuracy is 50 in urban and up to 300 meters in rural areas.
- **Assisted–GPS –** This is a combination of the previous method and GPS information, in case the GPS service is enabled. The average accuracy is 25 m in urban areas and up to 1 m in rural areas. Though the most accurate method, it requires active GPS connection, which may not always be present.

#### 2.4.3.4.Content-of-communication data

Under critical circumstances, the mobile operators can provide access to the real-time users' data flow to the authorized law enforcement agency perfoming a live investigation (in our study, this is the NLEA). The 3rd Generation Partnership Project (2014f) TS 33.106 standard has defined strict requirements for a legally compliant, network-assisted interception. 3GPP TS 33.106 enables lawfully authorized surveillance with the general system of interception (p. 8). In terms of the real-time evidence, 3rd Generation Partnership Project (2014f) refers to the service content as *Content-of-communication* (*CC*).The investigation, or the *Subject Based Interception* is invoked using a specific *Target Identity* (which essentially is the mobile user identification set).

On the basis, 3rd Generation Partnership Project (2014e) TS 33.107 specifies the architecture details, invocation functions and the handover interfaces. The interception invocation for circuit-switched services is defined for mobile-originated/terminated calls, call hold/waiting, multi-party calls, call forward/deflection, and explicit call transfer. On the packet core side, the interception is invoked relative to mobile station attach, location updates, PDP context activation and the IMS-related activities. The secure transfer of the acquired content is over defined *handover interfaces*. HI1 enables delivery and exchange of administrative information (warrants, authorizations, encryption keys, and target identity information), HI2 delivery of the interception related information (IRI); and HI3 delivery of the content-of-communication (CC).

## 2.5.Mobile-enabled Crime – Criminal Case Processing Perspective

The institutional analysis study of the mobile-enabled crime processing entails an exploration approach that rests on “the concept of social system” (Cole & Smith, 2006). Thus, the criminal justice system is examined on the way in which the organisation structure, institutional behavior, as well as legal processes, affect it as a social institution (Bell, 2006). Such an approach is useful because it explores how the justice delivery capacity and performance are perceived in the criminal justice arena. Aligned with the research problem, the answer to the research question is produced as an outcome of an institutional analysis of the mobile-enabled crime processing practice.

### 2.5.1. Societal Context of the Criminal Justice System

The criminal case processing possess the attributes of a *public good*, following that the judiciary must be “erected and maintained as a public institution” (Besanko & Braeutigam, 2010). While theoretically non-excludable, the allocation is restricted to the subjects involved in a given case, thus excluding other potential “consumers” for direct benefits of the particular judicial outcome. The limited resources are subtractable and may lead to congestion in circumstances of an excessive caseload in a given point of time, which makes it rivalrous in nature. Presuming maximum utilization, the criminal justice system prevents simultaneous allocation for other potential “consumers” in that particular moment. Thus, the justice allocation technically is not a pure public good, but rather a *quasi-public* good. The provision and production of this quasi-public good takes place in “complex criminal justice arrangements” (Aligica & Tarko, 2013, p. 726). The analysis of these arrangements necessitates an appropriate tool capable to diagnose the factors “threatening to destroy the resilience of the judicial system” (Ostrom, 2005). Fortunately, such a tool exists: called the Institutional Analysis and Development, this framework is chosen as a central analytical instrument for this research study.

### 2.5.2. Institutional Analysis of the Criminal Justice System – IAD Framework

The structure of the IAD framework, used as the main analytical instrument for this study, is depicted in Figure 5. At the core of the framework is the *action arena*, bringing the juristic context of the mobile-enabled crime processing in Macedonia, The action arena includes an *action situation*, that is, the mobile-enabled crime processing, and *actors* acting in delivering the justice. The analysis considers the *operational* tier or the actual mobile-enabled crime processing. It also considers the *collective-choice* tier, “where the judges are constrained by a set of collective-choice rules” (Ostrom, 2007). Figure 5 shows three institutional characteristics as inputs to the action arena. The rules-in-use are the legislative prescriptions about what actions are required, prohibited, or permitted in the processing of mobile-enabled crimes. The physical and material conditions determine the incentives of the actors and the resources available in handling mobile network data. Lastly, the attributes of a community are the cultural norms of behavior of the juristic actors. According to Ostrom (2007), they “affect the types of actions that can be taken and the likely outcomes achieved" when the crime is facilitated by the mobile service. The IAD analysis yielded the final research product in regards the contribution of the mobile network data on the case processing performance.

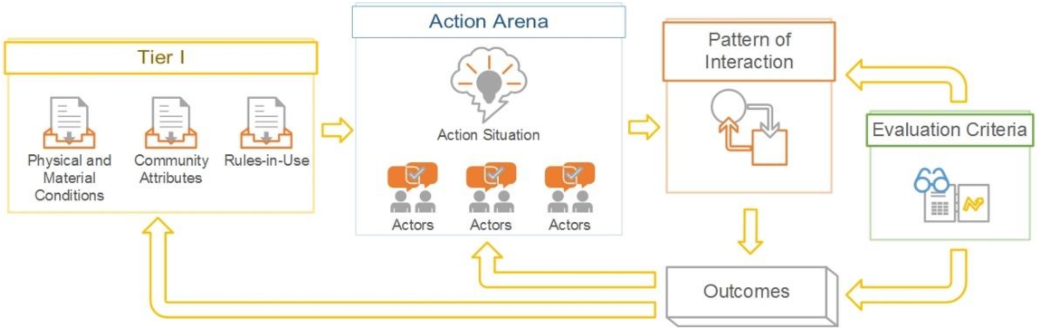


*Figure* 5. A Framework for Institutional Analysis. Source: Adapted from (Ostrom, 2007).

## 2.6.Summary

This chapter provided the background information used to answer the research question. The *anatomy of the Macedonian criminal justice system* section described its capacity to deliver criminal justice by reviewing the physical and material conditions, the community attributes and rules-in-use. The *performance of the Macedonian criminal justice system* section revealed how this capacity is utilized for an effective delivery of criminal justice as of the case disposition time. The following section brought the relationship between the basic and the mobile-enabled crime, reviewing the processes through which the *localization*, *network-management*, and *content-of-communication* data are involved as digital evidence in the criminal justice allocation. The structure of each of the mobile network data type was further elaborated in the subsequent section. Finally, the last one presented the analytical instrument used to execute this research study. The next chapter brings the methodology used to execute this research inquiry.

# CHAPTER 3. METHODOLOGY

This study explored the how the *localization*, *network-management* and *content-of-communication* data affect the criminal case processing in Macedonia. The research was designed as an *exploratory case study* seeking to understand whether and how the forensic management of these data types expedites the disposition time of the criminal cases where they have been included as evidence. To this objective, Figure 6 describes the main research concepts in coherence with the process of criminal justice delivery involving mobile network evidence.

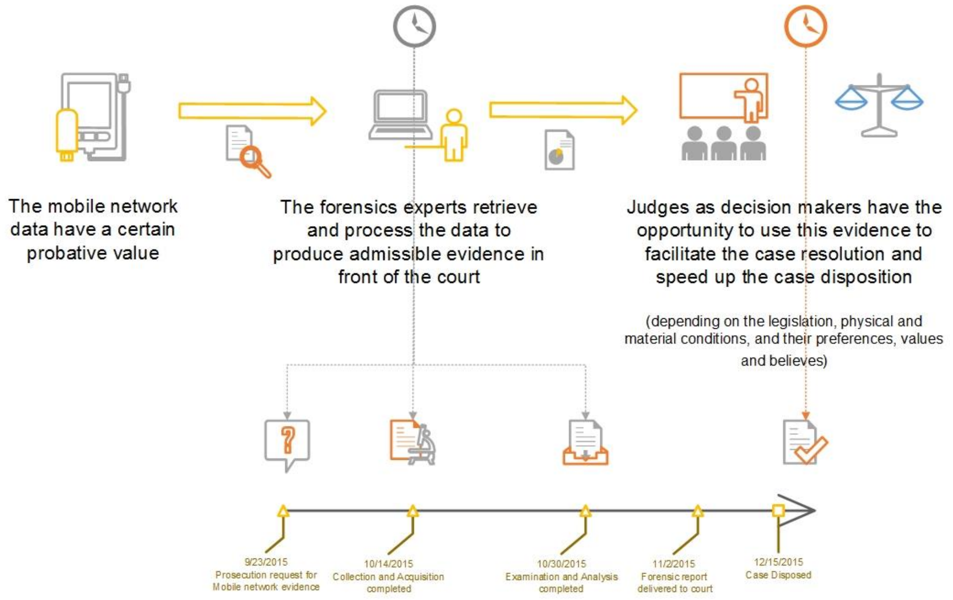

The mobile network data have a certain probative value
The forensics experts retrieve and process the data to produce admissible evidence in front of the court
Judges as decision makers have the opportunity to use this evidence to facilitate the case resolution and speed up the case disposition
(depending on the legislation, physical and material conditions, and their preferences, values and believes)
9/23/2015
Prosecution request for Mobile network evidence
10/14/2015
Collection and Acquisition completed
10/30/2015
Examination and Analysis completed
11/2/2015
Forensic report delivered to court
12/15/2015
Case Disposed

*Figure* 6. The research problem underpinning the exploratory case study.

The population of mobile-enabled crimes, the sampling method, and the sample itself used to answer the research question are defined under the data collection strategy. The data collection also encompasses the coding procedure yielding the independent, intervening and response variables together with their operational definitions. The approach for qualitative content analysis is described under the data analysis strategy, facilitating the central institutional analysis in regards the mobile network evidence contribution in the criminal case processing. Finally, this chapter provides the tactics for establishing the quality of the research inquiry methods.

## 3.1. Data Collection Strategy

The *entire population* of mobile-enabled crimes involves the criminal activities facilitated or committed using a mobile service from a 3GPP compliant operator or any violations of criminal law that involve knowledge of mobile technology for their perpetration, investigation, or prosecution. Because this study aimed to explain the contribution of the infrastructural data in processing the mobile-enabled crime, the sample population was comprised of those cases where the localization, mobile network-management, and content-of-communication data are included as juristic evidence. The *convenience sampling* was used to select mobile-enabled crime cases with a moderate amount of data as to provide enough time for codification and subsequent interpretation of the probative value of the associated evidentiary material. The sampling method accents mobile-enabled crimes within the local jurisdiction due to the legislative limitations in retrieving these data types from other jurisdictions. Thus, the sample of mobile-enabled crimes represents the local criminal segment in all the possible mobile-enabling contexts as of the aforementioned mobile data types.

The *first sampling criterion* was to select cases where the localization, network-management, and content-of-communication data can be included as a juristic evidence in moderate amount. Following the rules-in-use (section 2.1.3), all of these mobile network data types can be included as a juristic evidence when the criminal activity resides entirely under the *local* jurisdiction, while only the network-management data can be included when the criminal activity spans across multiple jurisdictions. Accordingly, the *second sampling criterion* was to further select cases from the local jurisdiction that include all mobile network data types and a multi-jurisdictional case that includes network-management data as a juristic evidence. Under the local jurisdiction, each mobile network data type can appear either as a standalone evidence or, the non-real time data - the localization and the network management data – can be combined with the content-of-communication data for the purpose of processing a given crime. Because the prosecution determines whether it needs to invoke a *standalone* or *combined* investigation to collect them, the *third selection criterion* – that being the investigation type – completed the convenience selection as such to include:

- One case with localization data retrieved from a standalone investigation
- One case with network-management data retrieved from a standalone investigation
- One case with content-of-communication data retrieved from a standalone investigation
- One case with localization data and content-of-communication data retrieved from a combined investigation

- One case with network-management data and content-of-communication data retrieved from a combined investigation
- One case with localization data, network-management data, and content-of-communication data retrieved from a combined investigation
- One multi-jurisdictional case that includes network-management data retrieved from a standalone investigation

Overall, the sample from the criminal case log of the Macedonian criminal justice system comprises of seven cases, noted as the *snapshot of mobile-enabled crimes*.

## 3.1.1. Mobile network evidence characteristics

### 3.1.1.1.Localization Data

To enable service delivery in a mobile fashion, the network periodically tracks users' location and exchanges signalization that supports accurate mobile service delivery. Because the perpetrators regularly use mobile service, the operator is able to provide a historical overview on their movement pattern – or the *localization data* - if such a thing is warranted as an evidence. The mobile service regulation requires the wireless coverage to be limited to the borders of the local (national) jurisdiction. Consequently, the localization data can be retrieved only by the home network of the user and only for the movement within these borders. To this point, three cases were selected to explore how the crime is reconstructed using the localization data (one as a single mobile data type, one combined with content-of-communication data, and one combined with both content-of-communication and network-management data) and whether the volume of the localization data or the combination with the other mobile data types (variety) have any impact on the case disposition time for the associated crime.

#### 3.1.1.2.Network-management Data

In instances where the service used by the perpetrator is of particular interest, the prosecution turns to the network operator to yield the *network-management data* that supported the realization of this service. Unlike the localization trace, the network-management data can be produced for the mobile users when they roam in visiting networks. Each visiting operator is responsible for transferring these data to the home operator for user management purposes. The prosecutors can look cross-territorially for such evidence if the criminal act spans multiple jurisdictions[2]. Because the network-management data informs on the nature and the chronological order of service activity, the sample includes cases with local and cross-territorial crimes for which this type of data were used as evidence in the case processing. Here the imperative was to explore how the crime is reconstructed using the service behavior profile developed using the network-management data and whether the volume, variety or the jurisdictional provenance have any impact on the case disposition time for the associated crimes.

#### 3.1.1.3.Content-of-Communication

The localization and network-management data provide the flexibility to be retrieved in a non-real time. That is, the time of evidence collection is not critical to preserve the evidence value, because the (home) operator is legally obliged to keep all of

[2] Although the European Convention on Cybercrime provides the legislative framework for network-management data delivery, there are no strict obligations for keeping network-management records on visiting activity, so the associated data might not be available from some operators or countries.

these records. However, given the real-time nature of the mobile service, there is a need to intercept time-critical content-of-communication, or the user data passing the network. For this purpose, the mobile operators enable interception taps to the National Law Enforcement Agency (NLEA). The content-of-communication can be intercepted only within the national borders (locally), because there is no regulative or legal possibility for a visiting traffic interception. Because the content-of-communication data can be used as a direct evidence, sometimes it is combined with the localization and/or network-management data to provide the associated geolocations and/or the service behavior. Therefore, the snapshot includes cases where different mobile network evidence is yielded with a combined investigation. The localization data together with the content-of-communication suggest where and for what purpose this communication occurred. The combination of network-management and content-of-communication data informs on mobile service behavior of the parties investigated. Finally, all three mobile network evidence types brings the most the network can provide for a given event of juristic interest. By taking a case with each of the respective combinations, the snapshot covers all the possible juristic contexts where the mobile data is relevant as evidence.

### 3.1.2. Sample Composition

Corresponding to the selection criteria, the *convenience sample* selected from the 2012/2013 case log of the Criminal Court of Macedonia is summarized in Table 1. The potential difficulties in this phase related to the actual availability of the sample cases, excessive evidence volume, or missing evidence/case log data. If a target sample cannot be completely retrieved from the archive, the most recent one was selected, equivalent to the respective scenario. In the event the access and case examination threatens to overwhelmingly prolong the collection, the next available sample with less voluminous evidence was selected. If a case was withhold for any reason, it was replaced with the next available that has the most recently acquired mobile network data.

Table 1. *Sample Composition - Mobile-Enabled Crimes*

| Case Sample | Jurisdiction | Investigation type | Mobile network data variety |
|---|---|---|---|
| 1 | Local | Standalone | Localization data |
| 2 | Local | Standalone | Network-management data |
| 3 | Local | Standalone | Content-of-communication data |
| 4 | Local | Combined | Localization and content-of-communication data |
| 5 | Local | Combined | Network-management and content-of-communication data |
| 6 | Local | Combined | Network-management, localization, and content-of-communication data |
| 7 | Multi | Standalone | Network-management data |

### 3.1.3. Research Variables

The collected case data encapsulate the jurisdictional-related and the investigation type-related selection criterions, determining the independent variables of interest for this study. Accordingly, the *independent variable set* consist of mobile network *variety* and *volume*, that is: the localization data – measured in number of localization records, network-management data – measured in number of network-management records, and content-of-communication data – measured in hours of intercepted conversations. Because the process of producing evidence out of the mobile network data (of any type) involves the forensics actions for its acquisition and delivery, followed by the actions for examination and analysis, two *intervening variables* were extracted from the forensic processing segment of the case data. The first one is associated with the evidence acquisition and delivery and is measured in days needed for the mobile network data (of any type and/or combination of types) to be transferred from the mobile network infrastructure into the forensics custody. The second one is associated with the examination and analysis and is measured in days needed for the mobile network evidence to be produced and reported to court. Both intervening variables affect the crime processing performance because the case disposition time – as the *response variable* measured in days needed for a criminal case to be brought to an end – aggregates them in the overall processing time for a given case. Table 2 summarizes the research variables as of the case data category and the data elements associated with each variable category.

Table 2. *Snapshot of Mobile-Enabled Crimes - Research Variables*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Evidence Variety | Localization Data | Number of localization records |
| | | Network-management Data | Number of network-management records |
| | | Content-of-communication | Hours |
| Intervening | Forensic processing | Acquisition and delivery time | Days |
| | | Analysis and examination time | Days |
| Response | Juristic processing | Disposition time | Days |

## 3.1.4. Operational Definition of the Research Variables

### 3.1.4.1.Independent Variables

The evidence variety incorporates the three types of mobile network data, that is, the localization data, the network-management data, and the content-of-communication data. Its effect is considered as the number of data types included in a case, that is, minimum variety (one data type), medium variety (two data types), and maximum variety (all three mobile network data types). As detailed in section 2.4., the localization data are comprised of so-called *localization records* that track mobile events as of their date, time, longitude, latitude and the target identity (or the observed MSISDN/IMSI/IMEI parameter in 3GPP vocabulary) to which they refer to. The network-management data consists of *network-management records* that track mobile events as of their date, time, type of service, dialed number / PDP address, and the target identity to which they refer to (or the observed MSISDN/IMSI/IMEI parameter in 3GPP vocabulary). The content-of-communication data consists of the intercepted conversations (or hours of conversational audio) for a given target identity (or the observed MSISDN/IMSI/IMEI parameter in 3GPP vocabulary) and include intercepted-related information records on the date, time, and dialed number of the conversations.

### 3.1.4.2.Intervening Variables

The *acquisition and delivery time* refers to the time needed for the mobile data to get into forensic custody. Because different mobile data types are acquired using different acquisition and delivery procedures, involve different actors, and the volume of localization/network-management records or content-of-communication hours can be different depending on the number of target identities investigated and the investigation timespan, the acquisition and delivery time varies from case to case and affects (by shortening or prolonging) the start of the forensic examination and analysis of the mobile data. On the same rationale, the forensics approach for examination and analysis is different for different mobile data types (or combination of them), requires different set of skills and competencies, and is impacted by the volume of the localization/network-management records or content-of-communication hours brought as a potential evidence, the *examination and analysis time* varies from case to case and affects (by shortening or prolonging) the production and reporting of the mobile network evidence in court.

#### 3.1.4.3.Response Variable

The response variable in this study is main case processing performance indicator used by the European Commission for the Efficiency of Justice, that is, the *case disposition time*. The case disposition time is the time that is needed to bring a case to an end and is measured in days. Essentially, it aggregates the days consumed for evidence retrieval and forensic processing in addition to the courtroom processing and the actions taken by the prosecution in developing a hypothesis on the crime. In other words, the criminal case processing performance is traced back to the forensic performance and with that, back to the mobile network data types, determining how their volume, variety and probative value contribute in the mobile-related crime case disposition.

## 3.2. Data Analysis Strategy

The data analysis strategy was to determine the relationship between the evidence-related information (the independent variable set), the forensic processing times (intervening variables) and the case disposition time (the response variable).
The first stage of the data analysis was a *content analysis* of the case material and the information on the Macedonian criminal justice case processing function reviewed in the second chapter. The second stage – or the IAD analysis - coupled the content analysis output with the contribution of the mobile network data as of the volume, variety and the forensic processing to observe the catalytic effect in the institutional settings of the Macedonian criminal justice system.

### 3.2.1. Content Analysis

The content analysis is summarized in the *exploratory matrix* in Figure 7. In the *first* cell, the case data were inspected to determine whether appropriate storage and distribution capabilities for a secure custody of the mobile network evidence are present in the Macedonian criminal justice system. In the *second* cell, the mobile network data included within the case data were inspected to determine the formats agreed in delivery of different mobile data types. In particular, these formats and the attributes included were compared with the 3GPP evidence formatting guidelines (section 2.3.2 and 2.4.3). Given that the convenience selection accent the local jurisdiction in all the mobile-enabling contexts, the analysis was set to reveal whether the network-management data delivered in the cross-jurisdictional case differs in formatting from the ones included in the local cases.

The case data were contrasted with the literature information from section 2.1.1 in the *third* cell to reveal the technical capacity available for presenting and utilizing the mobile network evidence (of any type) in the courtroom. The evidence delivery process was decomposed step-by-step in the *fourth* cell to reveal the actors and steps involved in the acquisition and delivery of different mobile data types. The training received in processing mobile-enabled crime cases according to the sections 2.3.1 and 2.3.2 was contrasted with this information to observe if any steps are taken to speed up this process (evidence triage, for example). Here, it must be noted that the auxiliary data on the mobile operator side (billing information, administrative metadata etc.) were not included within the content analysis.

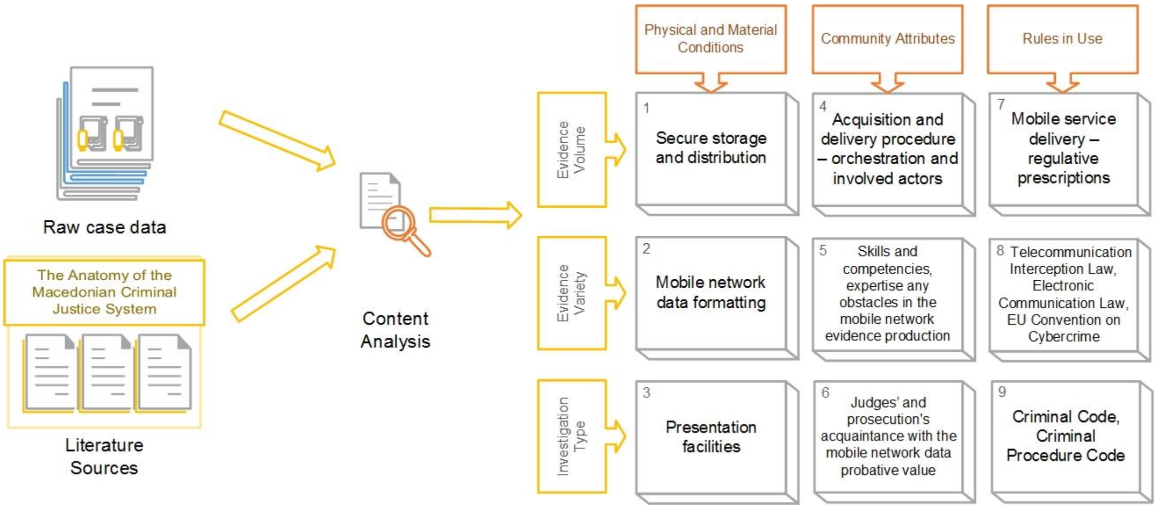

Raw case data
The Anatomy of the Macedonian Criminal Justice System
Literature Sources
Content Analysis
Physical and Material Conditions
Community Attributes
Rules in Use
Evidence Volume
Evidence Variety
Investigation Type
1 Secure storage and distribution
2 Mobile network data formatting
3 Presentation facilities
4 Acquisition and delivery procedure – orchestration and involved actors
5 Skills and competencies, expertise any obstacles in the mobile network evidence production
6 Judges' and prosecution's acquaintance with the mobile network data probative value
7 Mobile service delivery – regulative prescriptions
8 Telecommunication Interception Law, Electronic Communication Law, EU Convention on Cybercrime
9 Criminal Code, Criminal Procedure Code

*Figure* 7. The content analysis and the exploratory matrix.

In a similar vein, the case data was contrasted with the information from section 2.1.2, 2.3.1, 2.3.2 and 2.4.1 in the *fifth cell* to reveal the forensic methods for examination and analysis and the set of skills and competences required. This cell also inspected whether there were any financial-, technical-, or human-related obstacles in the forensic handling in the *fifth* cell. The *sixth* cell determined the level of acquaintance with the mobile technology by the judges and the prosecutors and their understanding of the associated probative value of mobile data types (or a combination of them) in accordance with the preferences, values and believes presented in sections 2.1.1.3 and 2.1.2.2.

As of the rules-in-use, the reports were reviewed in the *seventh* cell to reveal whether the associated 3GPP interfaces for administrative handling of mobile network evidence are implemented, namely the HI1 interface for authorization and authentication between the prosecution and the evidence delivery entity, the HI2 interface for delivery of the localization and network-management records, and the HI3 interface for delivery of the content-of-communication data. The content analysis in the *eight cell* detailed the mobile-enabled crime legislation regulating the forensic processing, that is:

- Electronic Communication Law, and the European Convention on Cybercrime (for the multi-jurisdictional case) – defining the roles, responsibilities and the procedures for acquisition and delivery, and the forensics examination and analysis of the localization and network-management data records.
- Telecommunication Interception Law - defining the roles, responsibilities and procedures for acquisition and delivery of the content-of-communication data (or the intercepted conversations)

Lastly, the content analysis in the *ninth cell* detailed the legislation framing the mobile-enabled crime processing within the Macedonian criminal justice system, or the Criminal Code (type of the mobile-related crime) and the Criminal Procedure Codes (investigation/evidence needed for its juristic processing).

### 3.2.2. IAD Analysis

The observations from the exploratory matrix were coupled with the information about the mobile network evidence production process to reveal the relationship between the forensic and judicial processing performance as depicted in Figure 8. They informed the IAD action arena with the detail trace on how the mobile network evidence traversed throughout the entire case cycle. The IAD analysis interpreted the relationship between the mobile network data variety and volume, and the acquisition and delivery time, the examination and analysis time, the juristic processing time, and the overall case disposition time in terms of the implication for action in the current practice and future research

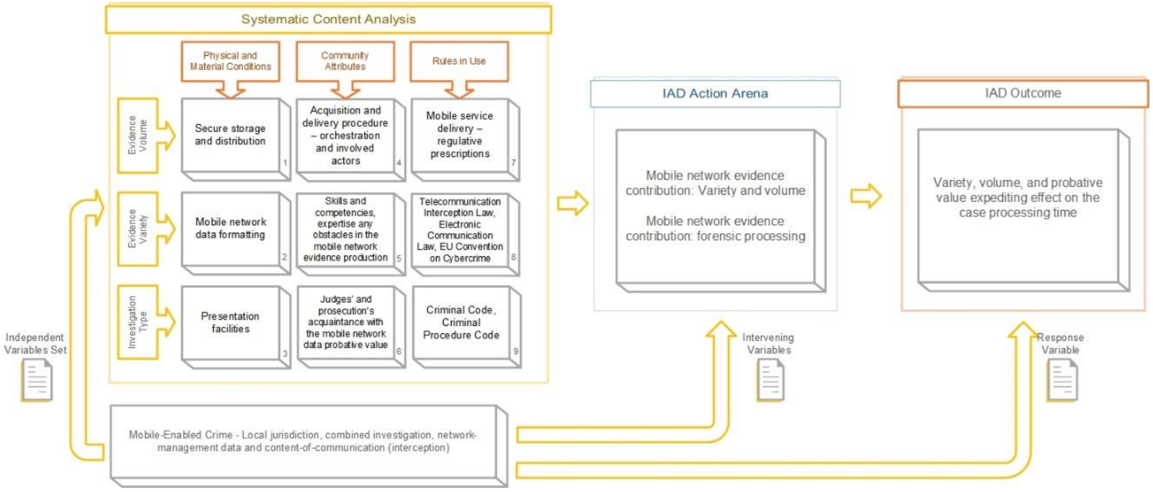

Systematic Content Analysis
Physical and Material Conditions
Community Attributes
Rules in Use
Evidence Volume
Evidence Variety
Investigation Type
Secure storage and distribution
1
Mobile network data formatting
2
Presentation facilities
3
Acquisition and delivery procedure – orchestration and involved actors
4
Skills and competencies, expertise any obstacles in the mobile network evidence production
5
Judges' and prosecution's acquaintance with the mobile network data probative value
6
Mobile service delivery – regulative prescriptions
7
Telecommunication Interception Law, Electronic Communication Law, EU Convention on Cybercrime
8
Criminal Code, Criminal Procedure Code
9
Independent Variables Set
Mobile-Enabled Crime - Local jurisdiction, combined investigation, network-management data and content-of-communication (interception)
IAD Action Arena
Mobile network evidence contribution: Variety and volume
Mobile network evidence contribution: forensic processing
Intervening Variables
IAD Outcome
Variety, volume, and probative value expediting effect on the case processing time
Response Variable

*Figure* 8. The IAD analysis.

### 3.3.Research Design Quality - Validity and Reliability

The quality of the study was established upon the *face validity* and *reliability* of the research design. The *face validity* test ascertains “that the research methods appear to be assessing the intended construct under study" (Phelan & Wren, 2002). *Reliability* refers to the "extent to which research findings can be replicated, assuming that the research methodology remains consistent" (Riege, 2003).

### 3.3.1. Face Validity

To ensure *face validity*, the research methods must capture the entire mobile network evidence contribution in the criminal case processing as of its catalytic effect. In other words, it must be shown that they are "obvious" in both forensics and judicial terms. Working backwards, the dependent variable yielded the judicial performance as per the European Commission for the Efficiency of Justice directives to which the Macedonian authorities also adhere. Thus, the IAD outcome is agreeable to the judicial stakeholders, given their familiarity with the case processing evaluation. This holds true also in forensics terms, because the intervening variables are de facto common performance indicators for the digital forensics practice (Casey, Ferraro, & Nguyen, 2009; Quick & Choo, 2014). Finally, the independent variables were operationalized and analyzed as per the globally standardized 3GPP terminology and recommendations.

### 3.3.2. Reliability

Traditionally, the research study is reliable to the extent it "demonstrates that the operations and procedures of the research inquiry can be repeated by other researchers which than achieve similar findings" (Merriam, 2009; Riege, 2003). In a formal sense, the replicability of this particular qualitative exploratory case study is challenging due to several reasons. First, the juristic decision-making and legal reasoning is not a straightforward formalistic process. Judges arrive at their decision not simply by applying the prescribed legal rules, but moreover they consider the mobile network evidence in a broader setting with the other evidence sources, testimonials, the parties involved in the crime, and the consequences incurred by their decision. That is, the mobile network data bring a formal discourse of the criminal reconstruction, but once presented in the courtroom, the associated criminal case is not immediately disposed. These factors influence the way judges perceive its probative value in conjunction with the remaining case data, which in turn, varies its catalytic effect on the case disposition performance.

Second, the forensic processing of the evidence is not a completely automated task too, because it depends on both the tacit and formal knowledge of the specialists, their experience, and the procedures/tools employed for acquisition, delivery, examination, and analysis of the mobile data types (or combination of). As noted, the crime reconstruction is formally discoursed by the interpretations on the mobile network data, however, when combined with another related evidence, there is a possibility that the final legal argument might differ from case to case even when the same type of mobile data is considered. Third, the physical and material conditions, the community attributes, and even the rules-in-use may change over time, so the explanatory matrix might be rendered differently at different points of time.

Although these arguments prevent establishing a traditional proof of reliability, there are also arguments favoring the structural consistency of the research inquiry. The content analysis and the operationalization of the independent variables are reliable by the fact that the mobile network data were categorized according to globally standardized guidelines for handling the associated evidence. Regardless of the number of instances or points in time a similar study is executed, the 3GPP mobile network data will yield the same format, structure, and pertinence to the criminal activities as provided in Table 2. For the intervening variables, the IAD analysis used the ISO SC27 guidelines when analyzing the forensic processing, so regardless of the investigation type, the evidence volume, and even the generation of mobile communication, the forensic engagement accordingly operationalized to the number of days consumed in data processing. The same holds true for the response variable, given that it is taken to be same with the key performance indicator for judicial performance assessment, developed and utilized by the European Commission for the Efficiency of Justice.

In addition to this, the IAD analysis itself aids both the replicability and the research consistency aspects of the study. The extensive amount of different studies in a diverse set of institutional problem domains (Ostrom, 2007) - all of them utilizing the IAD framework as the main analytical tool - assure that the findings are consistent with the institutional structure of the Macedonian criminal justice system, and moreover, that they can be replicated in terms of the relationship between the forensic and juristic processing of the mobile network evidence. Overall, the later arguments demonstrate that the research inquiry is stable and consistent in the overall structure of the research design. Most importantly, they assure that any future explorations of juristic contribution of mobile network data through an institutional prism will follow the systematic layout introduced and utilized by this particular study.

# CHAPTER 4. MOBILE-ENABLED CRIME PROCESSING ANALYSIS

In exploring the mobile network evidence contribution in the criminal case processing in Macedonia, seven cases were selected to render the relationship between the mobile network data volume and variety, the forensic handling times, and the overall case disposition time. Section 4.1 provides the information extracted from each case corresponding to the research variables of this study in accordance with the data collection strategy. Section 4.2 presents the descriptive statistics for the sample overall.

Following the data analysis strategy, section 4.3 presents the results from the statistical analysis of the relationship between the independent, intervening and the dependent variables. For the *mobile network data variety*, the analysis of variance tests and t-tests were performed respective to the acquisition and delivery time, the examination and analysis time, the juristic processing time, and the overall case disposition time. For the *mobile network data volume*, the aforementioned processing times were correlated with the number of localization records, the number of network-management records, and the hours of content-of-communication. The content analysis in section 4.4 reviews the statistical analysis results in conjunction with the remaining case information to complete the analysis of the mobile network data contribution in the case processing performance in Macedonia.

.

### 4.1. Case Data Elements - Research Operationalization

Table 3 summarizes the research data for the first criminal case, which included only localization data as mobile network evidence. Case I includes 7061 localization records that were acquired and delivered in 22 days and subsequently examined and analyzed in 35 days. The courtroom processing consumed 123 days and the case was disposed in 180 days overall.

Table 3.*Case I – Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Minimum Variety | Localization Data | Number of localization records = 7061 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 22 |
| | | Analysis and examination time | Days = 35 |
| Response | Case processing | Disposition time | Days = 180 |

Table 4 summarizes the research data for the second criminal case, which included only network-management data as mobile network evidence. Case II includes 68570 network-management records that were acquired and delivered in 9 days and subsequently examined and analyzed in 21 days. The courtroom processing consumed 55 days and the case was disposed in 85 days overall.

Table 4. *Case II – Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Minimum Variety | Network-management Data | Number of network-management records = 68570 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 9 |
| | | Analysis and examination time | Days = 21 |
| Response | Case processing | Disposition time | Days = 85 |

Table 5 summarizes the research data for the third criminal case, which included only content-of-communication data as mobile network evidence. Case III includes 300 hours of content-of-communication that were acquired and delivered in 7 days and subsequently examined and analyzed in 79 days. The courtroom processing consumed 357 days and the case was disposed in 443 days overall.

Table 5. *Case III – Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Minimum Variety | Content-of-communication | Hours = 300 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 7 |
| | | Analysis and examination time | Days = 79 |
| Response | Case processing | Disposition time | Days = 443 |

Table 6 summarizes the research data for the fourth criminal case, which included network-management and content-of-communication data as a mobile network evidence. Case IV includes 10305 network-management records and 14 hours of content-of-communication that were acquired and delivered in 14 days and subsequently examined and analyzed in 42 days. The courtroom processing consumed 179 days and the case was disposed in 235 days overall.

Table 6. *Case IV - Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Medium Variety | Network-management Data | Number of network-management records = 10305 |
| | | Content-of-communication | Hours = 14 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 14 |
| | | Analysis and examination time | Days = 42 |
| Response | Case processing | Disposition time | Days = 235 |

Table 7 summarizes the research data for the fifth criminal case, which included localization and content-of-communication data as a mobile network evidence. Case V includes 23216 localization records and 8 hours of content-of-communication that were acquired and delivered in 8 days and subsequently examined and analyzed in 32 days. The courtroom processing consumed 50 days and the case was disposed in 90 days overall.

Table 7. *Case V - Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Medium Variety | Localization Data | Localization records = 23216 |
| | | Content-of-communication | Hours = 8 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 8 |
| | | Analysis and examination time | Days = 32 |
| Response | Case processing | Disposition time | Days = 90 |

Table 8 summarizes the research data for the sixth criminal case, which included localization data, network-management data, and content-of-communication data as a mobile network evidence. Case VI includes 10300 localization records, 14207 network-management records, and 17 hours of content-of-communication that were acquired and delivered in 23 days and subsequently examined and analyzed in 75 days. The courtroom processing consumed 146 days and the case was disposed in 244 days overall.

Table 8. *Case VI- Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Maximum Variety | Localization Data | Number of localization records = 10300 |
| | | Network-management Data | Number of network-management records = 14207 |
| | | Content-of-communication | Hours = 17 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 23 |
| | | Analysis and examination time | Days = 75 |
| Response | Juristic processing | Disposition time | Days = 244 |

Table 9 summarizes the research data for the seventh criminal case, which included network-management data retrieved from multiple jurisdictions as a mobile network evidence. Case VII includes 72452 network-management records that were acquired and delivered in 22 days and subsequently examined and analyzed in 25 days. The courtroom processing consumed 59 days and the case was disposed in 106 days overall.

Table 9. *Case VII – Data Elements and Research Variables Values*

| Variables | Case Data | Data Elements | Operationalization |
|---|---|---|---|
| Independent | Minimum Variety | Network-management Data | Number of network-management records = 72452 |
| Intervening | Forensic processing | Acquisition and delivery time | Days = 22 |
| | | Analysis and examination time | Days = 25 |
| Response | Juristic processing | Disposition time | Days = 106 |

## 4.2. Case Data Summary – Descriptive Statistics

Table 10 and Table 11 display the descriptive statistics for the research variables presented in the previous subsection.

Table 10. *Sample's Descriptive Statistics for the Independent Variables*

| Category | Localization data | | Network-management data | | Content-of-communication data | |
|---|---|---|---|---|---|---|
| | Number of Records | N | Number of Records | N | Hours | N |
| Minimum | 7061 | 3 | 10305 | 4 | 8 | 4 |
| Maximum | 23216 | | 72452 | | 300 | |
| Average | 13525.66 | | 41386 | | 84.75 | |
| Median | 10300 | | 41393.5 | | 15.5 | |
| Σ | 8753.25 | | 32520.68 | | 111.15 | |

*The N indicates the number of cases in which the particular mobile network data types were included as mobile network evidence.*

Table 11. *Sample's Descriptive Statistics for the Intervening and Dependent Variable for N = 7 (the overall sample)*

| Category | Acquisition and delivery time | Examination and analysis time | Juristic Processing time* | Case disposition time |
|---|---|---|---|---|
| Minimum | 7 | 21 | 55 | 85 |
| Maximum | 23 | 79 | 345 | 443 |
| Average | 15 | 44.142 | 151.857 | 197.571 |
| Median | 14 | 35 | 144 | 180 |
| Σ | 7.21 | 23.47 | 101.45 | 118.337 |

**The final segment of the case processing process before the case is disposed. The case disposition time is a cumulative of the acquisition and delivery time, the examination and analysis time, and the juristic processing time.*

## 4.3. Case Data Analysis

The first three subsections display the independent, intervening, and the dependent variable for each case in the sample, respectively. Subsection 4.3.4 reports on the relationship between the *mobile network data variety* as independent variable and the intervening and dependent variables, presenting the outputs of the ANOVA tests and the t-tests for the minimum and medium variety cases (the maximum variety case was omitted for the t-tests because only Case VI includes all three mobile data types).

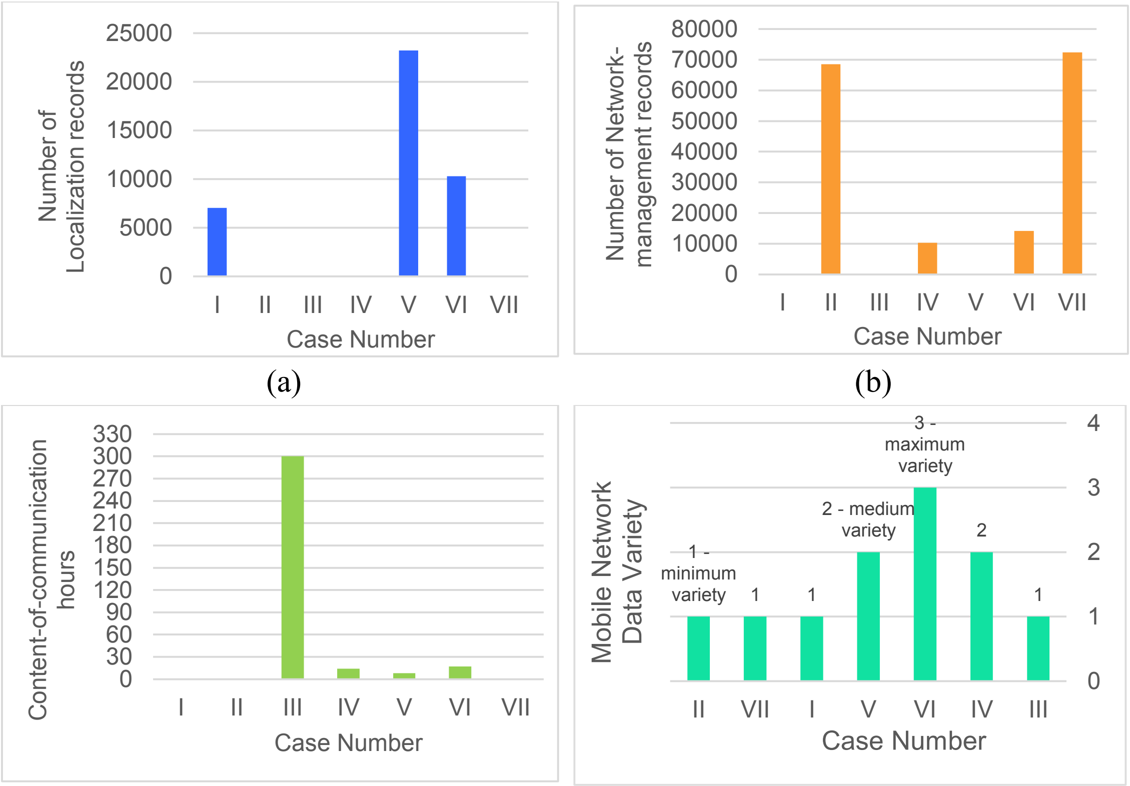
Accordingly, subsection 4.3.4.1 displays the relationship between the mobile network data variety and the *acquisition and delivery time* and subsection 4.3.4.2 the relationship between the mobile network data variety and the *examination and analysis time*. Because the dependent variable aggregates both of the intervening variables, the relationship between the mobile network data variety and the *juristic processing time* – the time spent on the juristic processing of the cases, or the case disposition time minus the compound forensics time - is presented in subsection 4.3.4.3. Subsection 4.3.4.4

reports on the relationship between the mobile network data variety and the *case disposition time*, and subsection 4.3.4.5 summarizes the *mobile network data variety* contribution in the case processing performance form the overall results.

Analogously, subsection 4.3.5 reports on the relationship between the *mobile network data volume* and the intervening and dependent variables, displaying the cross-value scatterplots and the correlational tables for each of the mobile network data types. Subsection 4.2.6 reports the relationship between the intervening and the dependent variable, with the cross-value scatterplots and the correlational tables for the acquisition and delivery time in subsection 4.2.6.1, the examination and analysis time in subsection 4.2.6.2, and the remaining juristic processing time in 4.2.6.3.

### 4.3.1. Independent Variables

Figure 9 displays the values of the independent variables. Figure 9 (a) depicts the number of localization records, 9(b) the number network-management records and 9(c) the hours of content-of-communication for each case. The zero values indicate that the particular mobile data type was not included in that case as an evidence. Figure 9(d) displays the mobile network data variety 1 that depicts cases with only one data type, 2 cases with two data types, and 3 cases with three data types.



(a)

(b)

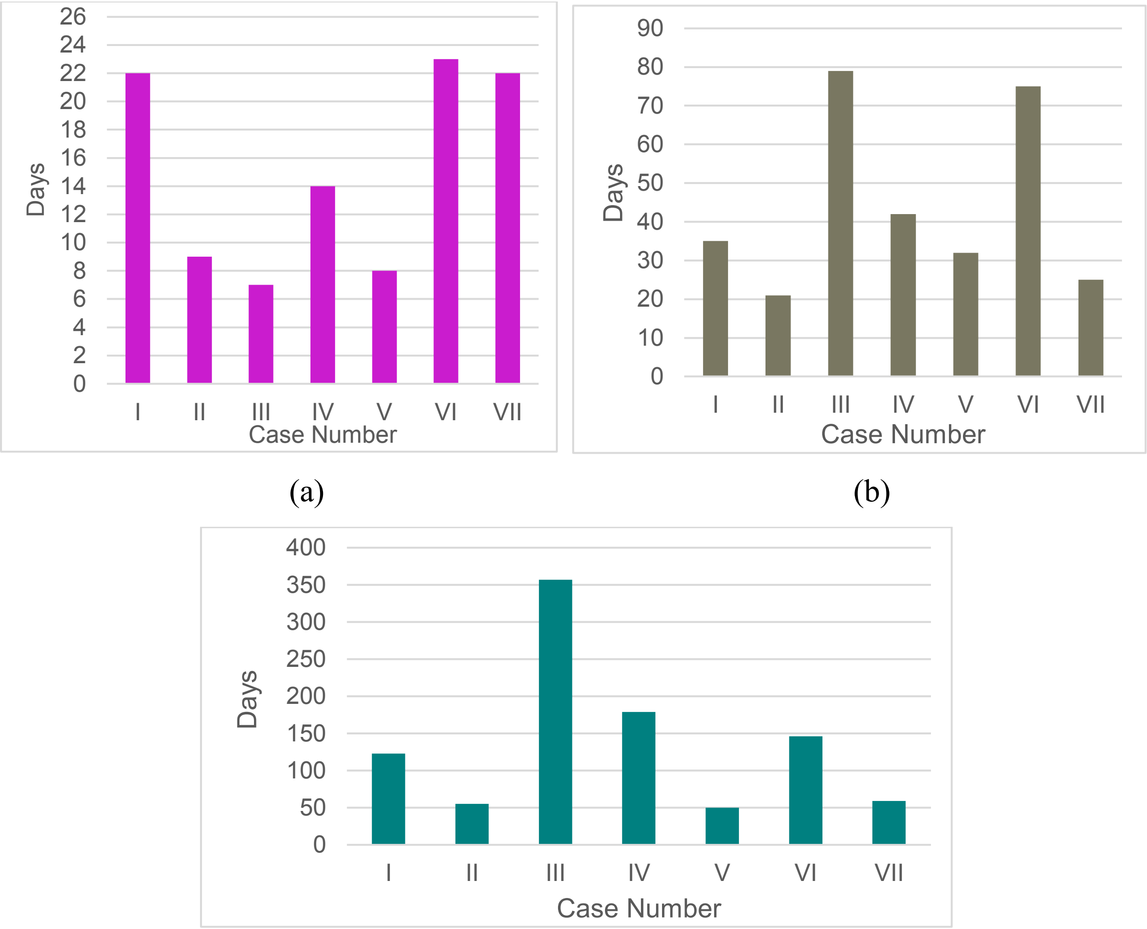
(c)

(d)

Figure 9. Independent variables: (a) Volume: Number of localization records. (b) Volume: Number of network-management records. (c) Volume: Hours of content-of-communication. (d) Mobile network data variety.

### 4.3.2. Intervening Variables

Figure 10 displays the values of the intervening variables. Figure 10(a) depicts the acquisition and delivery time, 10(b) the examination and analysis time, and 10(c) the remaining juristic processing time for each of the sample cases. Although not explicitly referred to in the overall research design in Chapter 3, the juristic processing time is displayed in Figure 10(c) as the remaining time of the overall case disposition time (minus the acquisition and delivery and the examination and analysis time).



(a)

(b)

(c)

Figure 10. The intervening variables' values for each case in the sample. (a) Number of acquisition and delivery days. (b) Number of examination and analysis days. (c) Juristic processing days.

### 4.3.3. Dependent Variables

Figure 11 depicts case disposition time for each case in the sample, aggregating the values presented in Figure 10(a), (b), and (c) in the previous subsection.

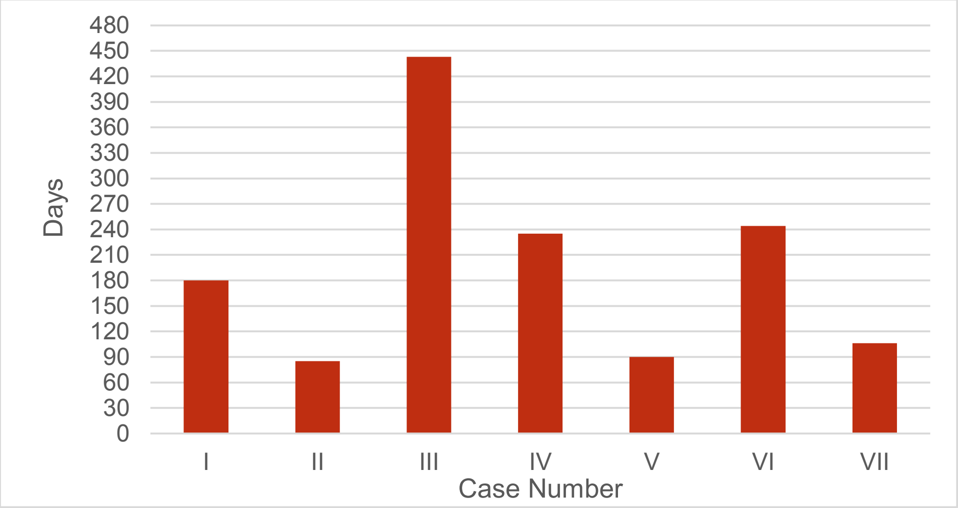


Figure 11. Case disposition days for each case in the sample.

### 4.3.4. Mobile Network Data Variety Contribution

The *mobile network data variety* contribution in the criminal case processing in the Macedonian criminal justice system is presented in this subsection.

#### 4.3.4.1. Mobile Network Data Variety and the Acquisition and Delivery Time

Figure 12 shows the relationship between the mobile network data variety and the *acquisition and delivery time*. Table 12 presents the ANOVA analysis with the descriptive values in Table 12(a), the homogeneity of the variance test in Table 12(b), and the ANOVA output in Table 12(c). Table 13 presents the t-test results between the cases with one and two mobile data types and the acquisition and delivery time, displaying the group statistics in Table 13(a) and the t-test output in Table 13(b).

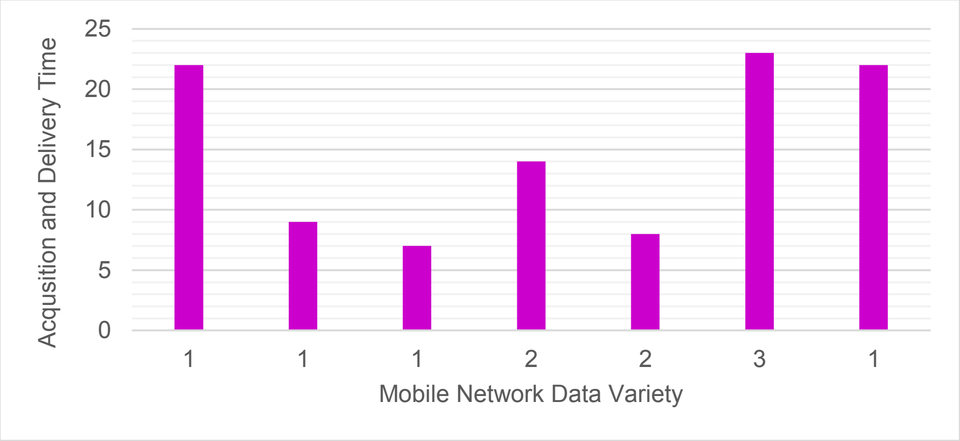


Figure 12. The cross-values of the mobile network data variety and the acquisition and delivery times for each case in the sample.

Table 12. *Mobile Network Data Variety and Acquisition and Delivery Time - **ANOVA**.*

(a) Descriptives

| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 1.00 | 4 | 15.0000 | 8.12404 | 4.06202 | 2.0728 | 27.9272 | 7.00 | 22.00 |
| 2.00 | 2 | 11.0000 | 4.24264 | 3.00000 | -27.1186 | 49.1186 | 8.00 | 14.00 |
| 3.00 | 1 | 23.0000 | . | . | . | . | 23.00 | 23.00 |
| Total | 7 | 15.0000 | 7.21110 | 2.72554 | 8.3308 | 21.6692 | 7.00 | 23.00 |

(b) Homogeneity of Variances

| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| 42.667[a] | 1 | 4 | .003 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Acquisition and Delivery Time.

(c) ANOVA Output

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 96.000 | 2 | 48.000 | .889 | .479 |
| Within Groups | 216.000 | 4 | 54.000 | | |
| Total | 312.000 | 6 | | | |

Table 13. *Mobile Data Network Variety and Acquisition and Delivery Time –* ***T-Test***.

(a) Group Statistics

| | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Acquisition and Delivery Time | 1.00 | 4 | 15.0000 | 8.12404 | 4.06202 |
| | 2.00 | 2 | 11.0000 | 4.24264 | 3.00000 |

(b) T-Test Output

**Independent Samples Test**

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | 95% Confidence Interval of the Difference | |
| | | | | | | | | | Lower | Upper |
| Acquisition and Delivery Time | Equal variances assumed | 42.667 | .003 | .629 | 4 | .564 | 4.00 | 6.364 | -13.669 | 21.669 |
| | Equal variances not assumed | | | .792 | 3.786 | .475 | 4.00 | 5.05 | -10.338 | 18.338 |

Considering the ANOVA and the t-test outputs from Table 12 and 13 - F (2, 4) = .889, p > .05 and t (7) = .792, p > .05 - it follows that the mobile network data variety has no impact on the acquisition and delivery time, neither in general terms nor for the subset of cases including one or two mobile data types. In other words, there are other factors that also affect the acquisition and delivery time (section 4.4 includes a discussion of these factors). However, it is worth noting the t-value of 0.792, because it suggests a larger acquisition and delivery time for cases with two mobile network data types compared with the cases including only one data type as an evidence.

#### 4.3.4.2. Mobile Network Data Variety and the Examination and Analysis Time

Figure 13 shows the relationship between the mobile network data variety and the *examination and analysis time*. Table 14 presents the ANOVA analysis with the descriptive values in Table 14(a), the homogeneity of the variance test in Table 14(b), and the ANOVA output in Table 14(c). Table 15 presents the t-test results between the cases with one and two mobile data types and the examination and analysis time, displaying the group statistics in Table 15(a) and the t-test output in Table 15(b).

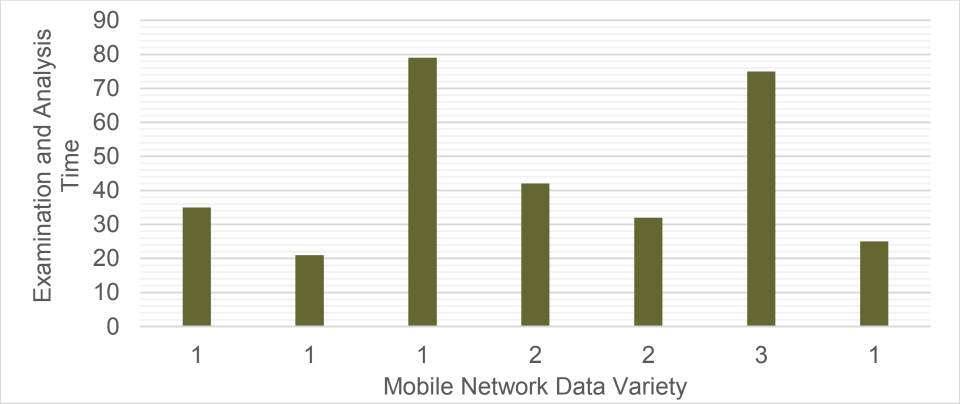
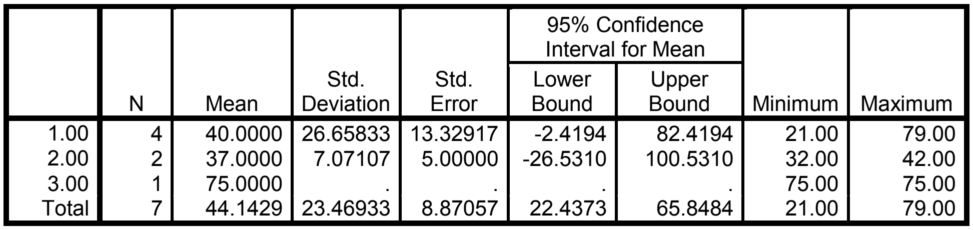


Figure 13. The cross-values of the mobile network data variety and the examination and analysis times for each case in the sample.

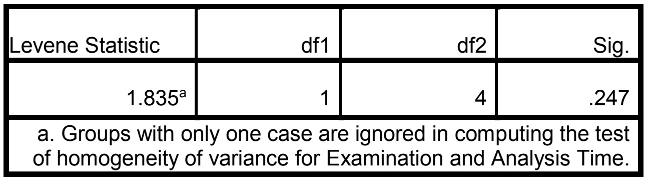
Table 14. *Mobile Network Data Variety and Examination and Analysis Time -* ***ANOVA***.

(a) Descriptives



| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 1.00 | 4 | 40.0000 | 26.65833 | 13.32917 | -2.4194 | 82.4194 | 21.00 | 79.00 |
| 2.00 | 2 | 37.0000 | 7.07107 | 5.00000 | -26.5310 | 100.5310 | 32.00 | 42.00 |
| 3.00 | 1 | 75.0000 | . | . | . | . | 75.00 | 75.00 |
| Total | 7 | 44.1429 | 23.46933 | 8.87057 | 22.4373 | 65.8484 | 21.00 | 79.00 |

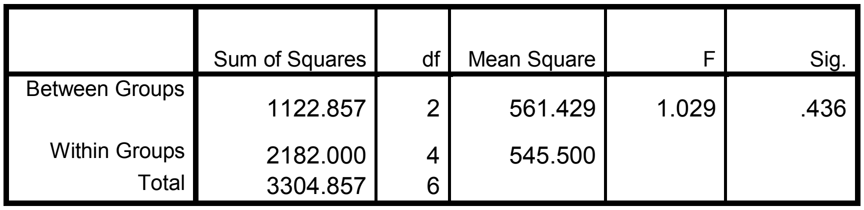
(b) Homogeneity of Variances



| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| 1.835[a] | 1 | 4 | .247 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Examination and Analysis Time.

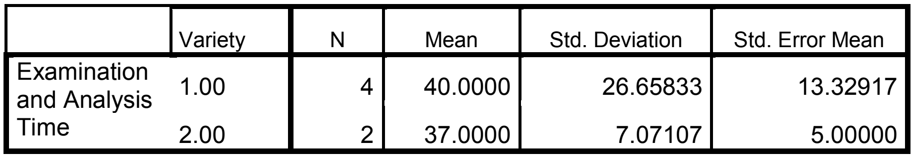
(c) ANOVA Output



| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 1122.857 | 2 | 561.429 | 1.029 | .436 |
| Within Groups | 2182.000 | 4 | 545.500 | | |
| Total | 3304.857 | 6 | | | |

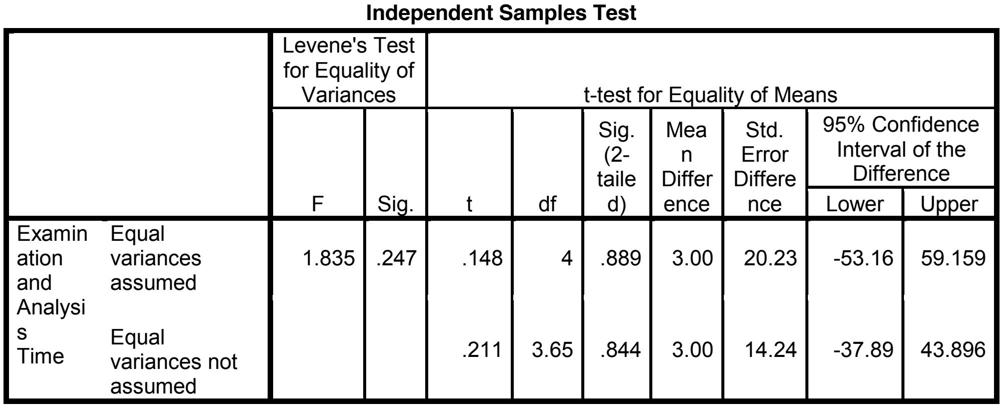
Table 15. *Mobile Network Data Variety and Examination and Analysis Time –* ***T-Test****.*

(a) Group Statistics



| | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Examination and Analysis Time | 1.00 | 4 | 40.0000 | 26.65833 | 13.32917 |
| | 2.00 | 2 | 37.0000 | 7.07107 | 5.00000 |

(b) T-Test Output



**Independent Samples Test**

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% Confidence Interval of the Difference | |
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| Examination and Analysis Time | Equal variances assumed | 1.835 | .247 | .148 | 4 | .889 | 3.00 | 20.23 | -53.16 | 59.159 |
| | Equal variances not assumed | | | .211 | 3.65 | .844 | 3.00 | 14.24 | -37.89 | 43.896 |

Considering the ANOVA and the t-test outputs from Table 14 and 15 - F (2, 4) = 1.029, p > .05 and t (7) = .148, p > .05 - it follows that the mobile network data variety has no impact on the examination and analysis time, neither in general terms nor for the subset of cases including one or two mobile data types. In other words, there are other factors that also affect the examination and analysis time in general (section 4.4 includes a discussion of these factors). However, it is worth noting the t-value of 0.148, because it suggests a relatively equal time dedicated for examination and analysis for all the cases regardless of the number of mobile network data types included as an evidence.

The analysis above was performed for the mobile network data variety instance without the Case III as an outlier and the *examination and analysis time*. Case III was removed to analyze the minimum variety as of the non-real time data, and the medium and maximum variety as a combination of non-real time and real time data. Figure 14 shows the relationship of the mobile network data variety and the examination and analysis time, Table 16 displays the ANOVA results, and Table 17 t-test results.

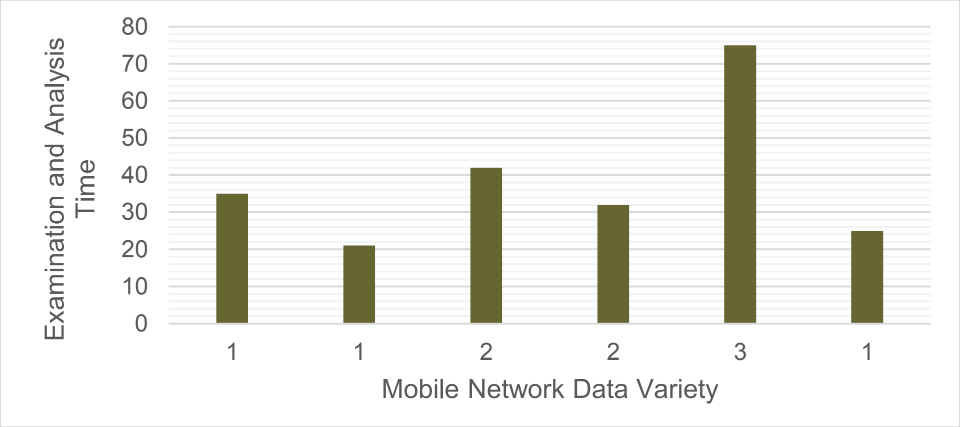


Figure 14. The cross-values of the mobile network data variety – without the outlier Case III - and the examination and analysis times for each case in the sample.

Table 16. *Mobile Network Data Variety and the Examination and Analysis Time (without the outlier Case III) -* ***ANOVA****.*

(a) Descriptives

| | | | | | 95% Confidence Interval for Mean | | | |
|---|---|---|---|---|---|---|---|---|
| | N | Mean | Std. Deviation | Std. Error | Lower Bound | Upper Bound | Minimum | Maximum |
| 1.00 | 3 | 27.0000 | 7.21110 | 4.16333 | 9.0866 | 44.9134 | 21.00 | 35.00 |
| 2.00 | 2 | 37.0000 | 7.07107 | 5.00000 | -26.5310 | 100.5310 | 32.00 | 42.00 |
| 3.00 | 1 | 75.0000 | . | . | . | . | 75.00 | 75.00 |
| Total | 6 | 38.3333 | 19.42850 | 7.93165 | 17.9444 | 58.7223 | 21.00 | 75.00 |

(b) Homogeneity of Variances

| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| .021[a] | 1 | 3 | .893 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Examination and Analysis Time.

(c) ANOVA Output

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 1733.333 | 2 | 866.667 | 16.883 | .023 |
| Within Groups | 154.000 | 3 | 51.333 | | |
| Total | 1887.333 | 5 | | | |

Table 17. *Mobile Network Data Variety and the Examination and Analysis Time (without the outlier Case III) – **T-Test**.*

(a) Group Statistics

| | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Examination and Analysis Time | 1.00 | 3 | 27.0000 | 7.21110 | 4.16333 |
| | 2.00 | 2 | 37.0000 | 7.07107 | 5.00000 |

(b) T-Test Output

**Independent Samples Test**

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% Confidence Interval of the Difference | |
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| Examination and Analysis Time | Equal variances assumed | .021 | .893 | -1.529 | 3 | .224 | -10 | 6.54 | -30.815 | 10.815 |
| | Equal variances not assumed | | | -1.537 | 2.31 | .248 | -10 | 6.51 | -34.671 | 14.671 |

In this instance, the ANOVA output is statistically significant with F (2, 3) = 16.883, p < .05 (p = 0.023) while the t-test remains insignificant, t (7) = -1.529, p > .05, on the account of the removed Case III that contains only content-of-communication data. This suggests that for the reduced sample without the maximum volume case of content-of-communication data, the mobile network data variety affects the examination and analysis time. However, the insufficient number of maximum variety cases (only one) prevents performing a post-hoc analysis to determine the exact relationship between the examination and analysis time and the number of mobile data types included as evidence. Again, the large t-value is worth noting in the context of the forensics effort, indicating interesting difference in the forensic processing for the cases where there is only localization or network-management data versus when they are combined with the content-of-communication data.

4.3.4.3.Mobile Network Data Variety and the Juristic Processing Time

Figure 15 shows the relationship between the mobile network data variety and the *juristic processing time*. Table 18 presents the ANOVA results with the descriptive values in Table 18(a), the homogeneity of the variance test in Table 18(b), and the ANOVA output in Table 18(c). Table 19 presents the t-test results between the cases with one and two mobile data types and the juristic processing time, displaying the group statistics in Table 19(a) and the t-test output in Table 19(b).

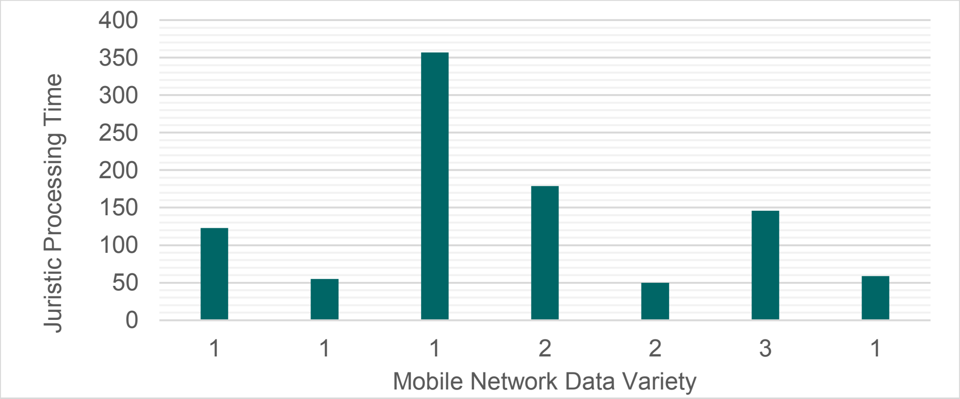


Figure 15. The cross-values of the mobile network data variety and the juristic processing times for each case in the sample.

Table 18. *Mobile Network Data Variety and the Juristic Processing Time - **ANOVA**.*

(a) Descriptives

| | | | | | 95% Confidence Interval for Mean | | | |
|---|---|---|---|---|---|---|---|---|
| | N | Mean | Std. Deviation | Std. Error | Lower Bound | Upper Bound | Minimum | Maximum |
| 1.00 | 4 | 148.5000 | 142.4488 | 71.22441 | -78.1679 | 375.1679 | 55.00 | 357.00 |
| 2.00 | 2 | 161.5000 | 24.74874 | 17.50000 | -60.8586 | 383.8586 | 144.00 | 179.00 |
| 3.00 | 1 | 146.0000 | . | . | . | . | 146.00 | 146.00 |
| Total | 7 | 151.8571 | 101.4502 | 38.34457 | 58.0314 | 245.6829 | 55.00 | 357.00 |

(b) Homogeneity of Variances

| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| 2.306[a] | 1 | 4 | .203 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Juristic Processing Time.

(c) ANOVA Output

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 265.357 | 2 | 132.679 | .009 | .991 |
| Within Groups | 61487.500 | 4 | 15371.875 | | |
| Total | 61752.857 | 6 | | | |

Table 19. *Mobile Network Data Variety and the Juristic Processing Time – **T-Test**.*

(a) Group Statistics

| | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Juristic Processing Time | 1.00 | 4 | 148.5000 | 142.44882 | 71.22441 |
| | 2.00 | 2 | 161.5000 | 24.74874 | 17.50000 |

(b) T-Test Output

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% Confidence Interval of the Difference | |
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| Juristic Processing Time | Equal variances assumed | 2.306 | .203 | -.121 | 4 | .909 | -13 | 107.38 | -311.11 | 285.11 |
| | Equal variances not assumed | | | -.177 | 3.337 | .870 | -13 | 73.343 | -233.64 | 207.64 |

Considering the ANOVA and the t-test outputs from Table 18 and 19 - F (2, 4) = .009, p > .05 and t (7) = -.121, p > .05 - it follows that the mobile network data variety has no impact on the juristic processing time too, neither in general terms nor in the subset of cases including one or two mobile data types. In other words, there are other factors that also affect the juristic processing time (section 4.4 includes discussion of these factors). However, it is worth noting the t-value of -0.121, because it suggests a relative equal time dedicated for the juristic processing for all the cases regardless of the number of mobile network data types included as an evidence.

4.3.4.4. Mobile Network Data Variety and the Case Disposition Time

Figure 16 shows the relationship between the mobile network data variety and the case disposition time. Table 20 presents the ANOVA analysis with the descriptives values in Table 20(a), the homogeneity of the variance test in Table 20(b), and the ANOVA output in Table 20(c). Table 21 presents the t-test results between the cases with one and two mobile data types and the case disposition time, displaying the group statistics in Table 21(a) and the t-test output in Table 21(b).

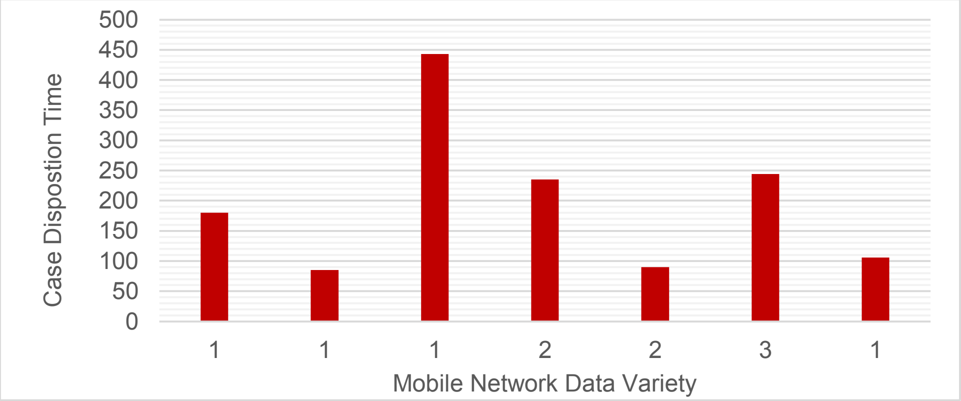


Figure 16. The cross-values of the mobile network data variety and the case disposition times for each case in the sample.

Table 20. *Mobile Network Data Variety and the Case Disposition Time -* ***ANOVA***.

(a) Descriptives

| | N | Mean | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | | Minimum | Maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower Bound | Upper Bound | | |
| 1.00 | 4 | 203.5000 | 164.7837 | 82.39185 | -58.7076 | 465.7076 | 85.00 | 443.00 |
| 2.00 | 2 | 209.5000 | 36.06245 | 25.50000 | -114.5082 | 533.5082 | 184.00 | 235.00 |
| 3.00 | 1 | 244.0000 | . | . | . | . | 244.00 | 244.00 |
| Total | 7 | 211.0000 | 118.3779 | 44.74265 | 101.5187 | 320.4813 | 85.00 | 443.00 |

(b) Homogeneity of Variances

| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| 1.966a | 1 | 4 | .234 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Case Disposition Time.

(c) ANOVA Output

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 1318.500 | 2 | 659.250 | .032 | .969 |
| Within Groups | 82761.500 | 4 | 20690.375 | | |
| Total | 84080.000 | 6 | | | |

Table 21. *Mobile Network Data Variety and the Case Disposition Time –* ***T-Test***.

(a) Group Statistics

| | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Case Disposition Time | 1.00 | 4 | 203.5000 | 164.78370 | 82.39185 |
| | 2.00 | 2 | 209.5000 | 36.06245 | 25.50000 |

(b) T-Test Output

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | 95% Confidence Interval of the Difference | |
| | | | | | | | | | Lower | Upper |
| Case Disposition Time | Equal variances assumed | 1.966 | .234 | -.048 | 4 | .964 | -6 | 124.57039 | -351.86 | 339.86 |
| | Equal variances not assumed | | | -.070 | 3.506 | .948 | -6 | 86.248 | -259.38 | 247.38 |

Considering the ANOVA and the t-test outputs from Table 20 and 21 - F (2, 4) = .032, p > .05 and t (7) = -.048, p > .05 - it follows that the mobile network data variety has no impact on the case disposition time too, neither in general terms nor in the subset of cases including one or two mobile data types. In other words, there are other factors that also affect the case disposition time (section 4.4 includes a discussion of these factors). Again, it is worth noting the absolute t-value of -0.048, because it suggests a relatively equal case processing effort for all the cases regardless of the number of mobile network data types included as evidence. In other words, the mobile network data variety – considered in the narrow terms of just the number of mobile data types in one case - does not have any significant impact on the case processing performance, per se.

The impact of the mobile network data variety on the case disposition time was also analyzed without the Case III as the outlier with the most outstanding value among all the cases in terms overall days of case processing (case disposition time = 443 days). Figure 17 shows the relationship between the mobile network data types and the case disposition time, Table 22 the ANOVA results, and Table 33 the t-test results.

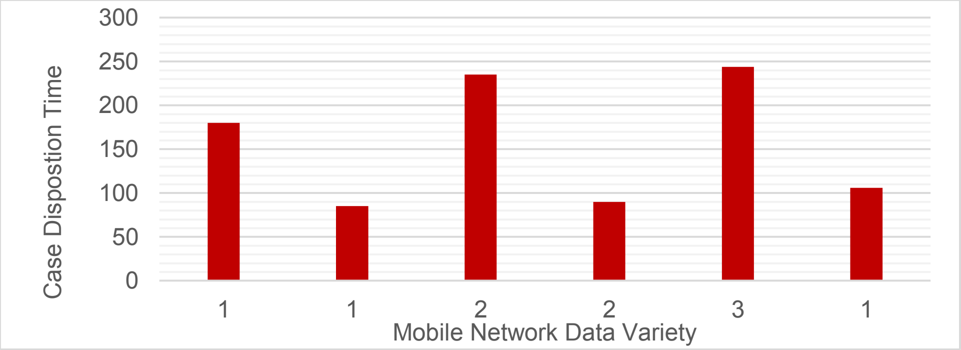


Figure 17. The cross-values of the mobile network data variety – without the outlier Case III - and the case disposition times for each case in the sample.

Table 22. *Mobile Network Data Variety and the Case Disposition Time (without the outlier Case III) -* ***ANOVA***.

(a) Descriptives

|  |  |  |  |  | 95% Confidence Interval for Mean |  |  |  |
|---|---|---|---|---|---|---|---|---|
|  | N | Mean | Std. Deviation | Std. Error | Lower Bound | Upper Bound | Minimum | Maximum |
| 1.00 | 3 | 123.6667 | 49.90324 | 28.81165 | -.2999 | 247.6332 | 85.00 | 180.00 |
| 2.00 | 2 | 209.5000 | 36.06245 | 25.50000 | -114.508 | 533.5082 | 184.00 | 235.00 |
| 3.00 | 1 | 244.0000 | . | . | . | . | 244.00 | 244.00 |
| Total | 6 | 172.3333 | 65.24620 | 26.63665 | 103.8616 | 240.8050 | 85.00 | 244.00 |

(b) Homogeneity of Variances

| Levene Statistic | df1 | df2 | Sig. |
|---|---|---|---|
| .698a | 1 | 3 | .465 |

a. Groups with only one case are ignored in computing the test of homogeneity of variance for Case Disposition Time.

(c) ANOVA Output

|  | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 15004.167 | 2 | 7502.083 | 3.583 | .160 |
| Within Groups | 6281.167 | 3 | 2093.722 |  |  |
| Total | 21285.333 | 5 |  |  |  |

Table 23. *Mobile Network Data Variety and the Case Disposition Time (without the outlier Case III) –* ***T-Test***.

(a) Group Statistics

|  | Variety | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Case Disposition Time | 1.00 | 3 | 123.6667 | 49.90324 | 28.81165 |
|  | 2.00 | 2 | 209.5000 | 36.06245 | 25.50000 |

(b) T-Test Output

|  |  | Levene's Test for Equality of Variances |  | t-test for Equality of Means |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  | 95% Confidence Interval of the Difference |  |
|  |  | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| Case Disposition Time | Equal variances assumed | .698 | .465 | -2.055 | 3 | .132 | -85.83333 | 41.77 | -218.76 | 47.099 |
|  | Equal variances not assumed |  |  | -2.231 | 2.856 | .116 | -85.83333 | 38.47 | -211.85 | 40.185 |

With the ANOVA and the t-test outputs of F (2, 3) = 3.583, p > .05 and t (6) = -2.055, p > .05 – there are no changes in regards the mobile network data variety impact on the case disposition time, even in the case when the extreme case is removed. What is worth mentioning is the interesting difference in the forensic processing for the cases where there is only localization or network-management data versus when they are combined with the content-of-communication data. In conjunction with the similar observation yielded for the examination and analysis time, this suggests a potential correlation between the forensic processing performance and the overall case processing performance (section 4.3.6 includes the results for this correlation).

#### 4.3.4.5. Mobile Network Data Variety and the Case Processing Performance - Summary

The mobile network data variety – considered in the narrow terms of just the number of mobile data types included in one case - does not have any significant impact on the case processing performance, per se. The results indicate a larger acquisition and delivery time for cases with two mobile network data types compared with the cases including only one data type as an evidence. An interesting difference is noticed in the forensic processing for the cases where there are only localization or network-management data versus when they are combined with the content-of-communication data. The same difference is also noticed for the overall case processing performance. The extended analysis for the mobile network data variety and the examination and analysis time without the outlier Case III yielded a statistically significant ANOVA output, suggesting a potential impact of the mobile network data variety on the forensic processing. However, the smaller sample size prevented a further post-hoc analysis to explore this impact in more details.

Notwithstanding the statistical insignificance, the results show that the mobile network data variety plays a significant role in the part of the case disposition time where the probative value is actually extracted, being that of principal interest for the juristic actors. Therefore, the analysis considered the effect of the forensic processing times and the juristic processing time on the case disposition time in section 4.3.6.

### 4.3.5. Mobile Network Data Volume Contribution

The *mobile network data volume* contribution in the criminal case processing in the Macedonian criminal justice system is presented in this subsection.

#### 4.3.5.1. Mobile Network Data Volume and the Acquisition and Delivery Time

##### 4.3.5.1.1. Localization Data

Figure 18 shows the number of localization data records on the x-axis and the acquisition and delivery time on the y-axis. The corresponding correlational table is displayed in Table 24, *r* = -.969, p > .05. Although there is no significant correlation between the number of localization data records and the acquisition and delivery time, it is worth noting the high negative value of the Pearson’s coefficient, that is, the negative relationship between the volume and the time needed the localization records to be brought in forensic custody.

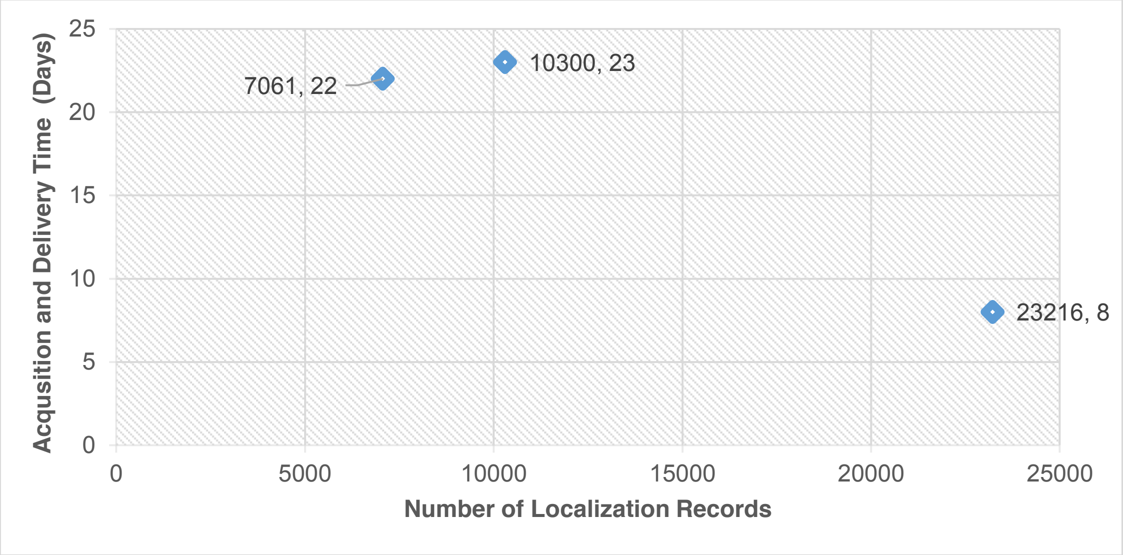


Figure 18. The number of localization records and the acquisition and delivery time.

Table 24. *Number of Localization Data Records and the Acquisition and Delivery Time – **Correlation**.*

| | | Acquisition and Delivery Time | No. of Localization Records |
|---|---|---|---|
| Acquisition and Delivery Time | Pearson Correlation | 1 | -.969 |
| | Sig. (2-tailed) | | .159 |
| | N | 3 | 3 |
| No. of Localization Records | Pearson Correlation | -.969 | 1 |
| | Sig. (2-tailed) | .159 | |
| | N | 3 | 7 |

### 4.3.5.1.2. Network-management Data

Figure 19 shows the number of network-management data records on the x-axis and the acquisition and delivery time on the y-axis. The corresponding correlational table is displayed in Table 25, *r* = -.195, p > .05. Although there is no significant correlation between the number of network-management data records and the acquisition and delivery time, it is worth noting the negative value of the Pearson's coefficient, that is, the negative relationship between the volume and the time needed the network-management records to be brought in forensic custody. Having a similar observation also for the localization data, it follows that the inversely proportional trend between the volume and the acquisition and delivery time is characteristic for the non-real time mobile network data types.

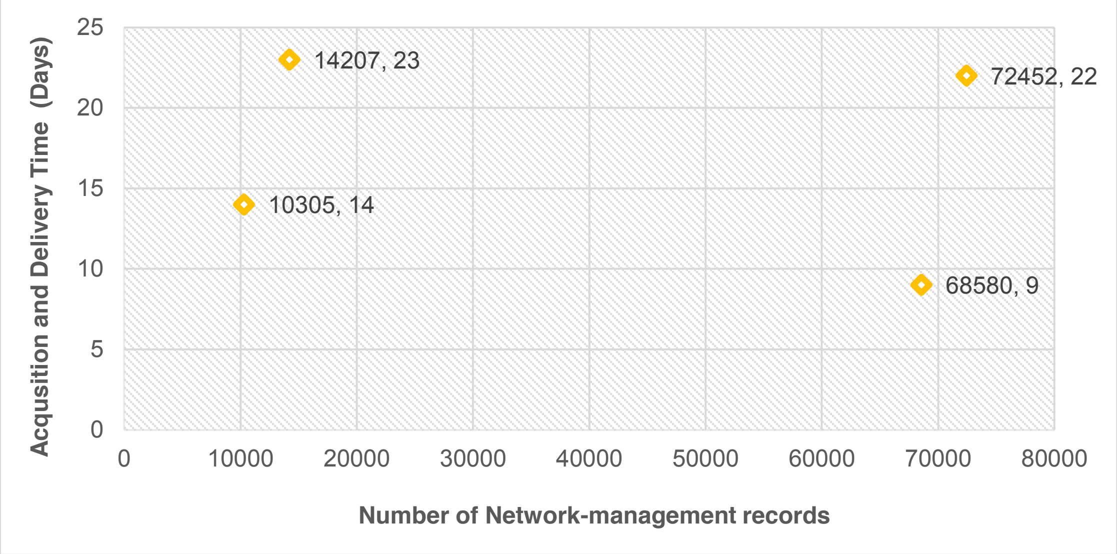


Figure 19. The number of network-management records and the acquisition and delivery time.

Table 25. *Number of Network-management Data Records and the Acquisition and Delivery Time – **Correlation***.

| | | Acquisition and Delivery Time | No. of Network-management Records |
|---|---|---|---|
| Acquisition and Delivery Time | Pearson Correlation | 1 | -.195 |
| | Sig. (2-tailed) | | .805 |
| | N | 4 | 4 |
| No. of Network-management Records | Pearson Correlation | -.195 | 1 |
| | Sig. (2-tailed) | .805 | |
| | N | 4 | 7 |

4.3.5.1.3. Content-of-communication Data

Figure 20 shows the number of content-of-communication hours on the x-axis and the acquisition and delivery time on the y-axis. The corresponding correlational table is displayed in Table 26, *r* = -.523, p > .05. Considering the negative Pearson's coefficient in conjunction with the foregoing observations, if follows that the negative relationship between the volume and the acquisition and delivery time is characteristic for all mobile network data types, including the content-of-communication data.

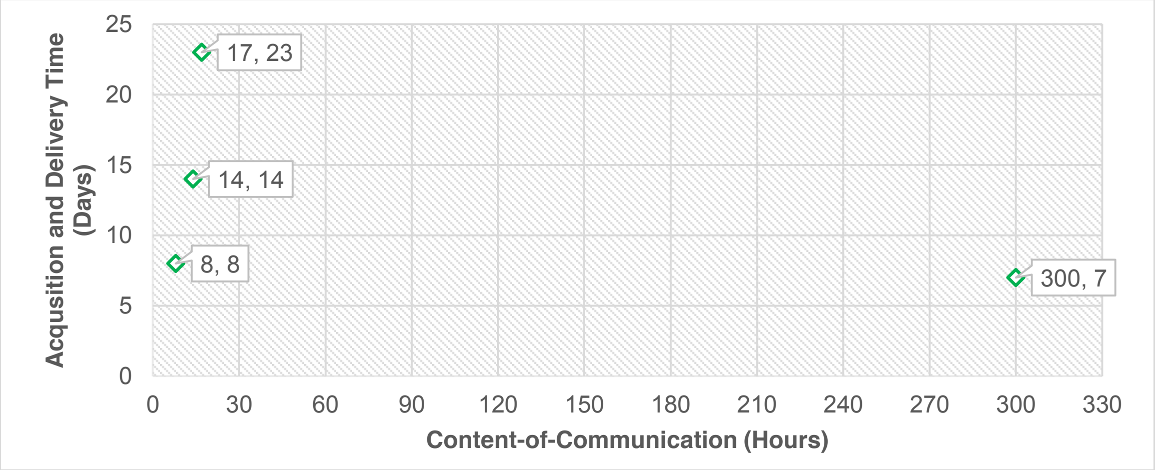


Figure 20. The hours of content-of-communication data and the acquisition and delivery time.

Table 26. *Hours of Content-of-communication and the Acquisition and Delivery Time – **Correlation***.

| | | Acquisition and Delivery Time | Hours of Content-of-communication |
|---|---|---|---|
| Acquisition and Delivery Time | Pearson Correlation | 1 | -.523 |
| | Sig. (2-tailed) | | .477 |
| | N | 4 | 4 |
| Hours of Content-of-communication | Pearson Correlation | -.523 | 1 |
| | Sig. (2-tailed) | .477 | |
| | N | 4 | 7 |

### 4.3.5.2. Mobile Network Data Volume and the Examination and Analysis Time

#### 4.3.5.2.1. Localization Data

Figure 21 shows the number of localization data records on the x-axis and the examination and analysis time on the y-axis. The corresponding correlational table is displayed in Table 27, *r* = -.385, p > .05. Although there is no significant correlation between the number of localization data records and the examination and analysis time, again it is worth noting the high negative value of the Pearson's coefficient, that is, the negative relationship between the volume and the time needed the localization records to be forensically processed.

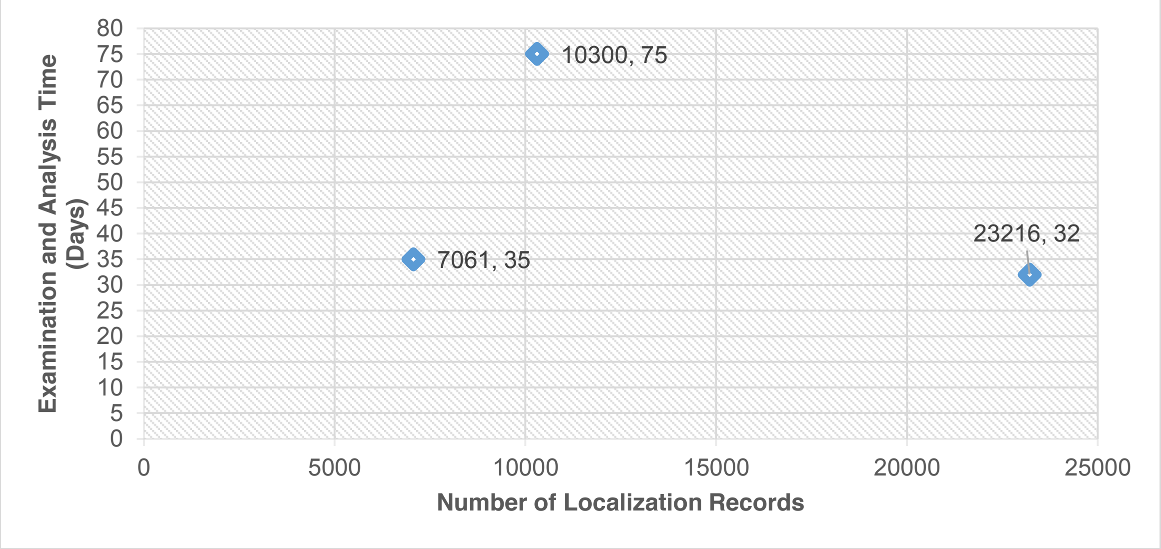


Figure 21. The number of localization records and the examination and analysis time.

Table 27. *Number of Localization Data Records and the Examination and Analysis Time – **Correlation**.*

| | | Examination and Analysis Time | No. of Localization Records |
|---|---|---|---|
| Examination and Analysis Time | Pearson Correlation | 1 | -.385 |
| | Sig. (2-tailed) | | .748 |
| | N | 3 | 3 |
| No. of Localization Records | Pearson Correlation | -.385 | 1 |
| | Sig. (2-tailed) | .748 | |
| | N | 3 | 7 |

4.3.5.2.2. Network-management Data

Figure 22 shows the number of network-management data records on the x-axis and the examination and analysis time on the y-axis. The corresponding correlational table is displayed in Table 28, *r* = -.803, p > .05. Having a negative Pearson's coefficient also for the network-management data, a negative relationship between the volume and the time needed for forensic processing can be observed for the non-real time mobile network data types in broader terms.

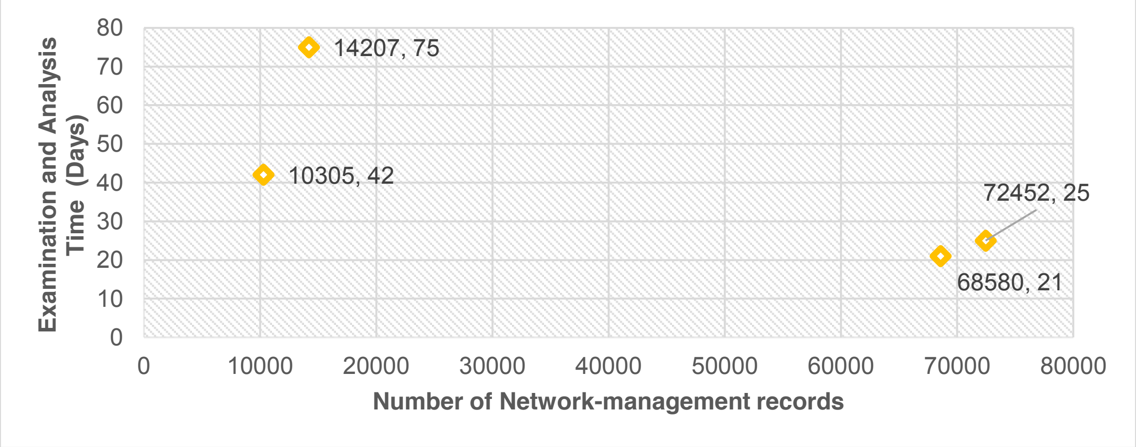


Figure 22. The number of network-management records and the examination and analysis time.

Table 28. *Number of Network-management Data Records and the Examination and Analysis Time –* ***Correlation****.*

| | | Examination and Analysis Time | No. of Network-management Records |
|---|---|---|---|
| Examination and Analysis Time | Pearson Correlation | 1 | -.803 |
| | Sig. (2-tailed) | | .197 |
| | N | 4 | 4 |
| No. of Network-management Records | Pearson Correlation | -.803 | 1 |
| | Sig. (2-tailed) | .197 | |
| | N | 4 | 7 |

4.3.5.2.3. Content-of-communication Data

Figure 23 shows the scatterplot depicting the number of content-of-communication hours on the x-axis and the examination and analysis time on the y-axis. The corresponding correlational table is displayed in Table 29, *r* = .642, p > .05. In contrast to the non-real time data, the Pearson's coefficient for the real-time data type or the content-of-communication is positive in this case, again still bearing that the statistical significance is not achieved due to the small sample size. In forensic processing terms, this translates in a positive relationship between the hours of intercepted data and the time needed to be examined and analyzed.

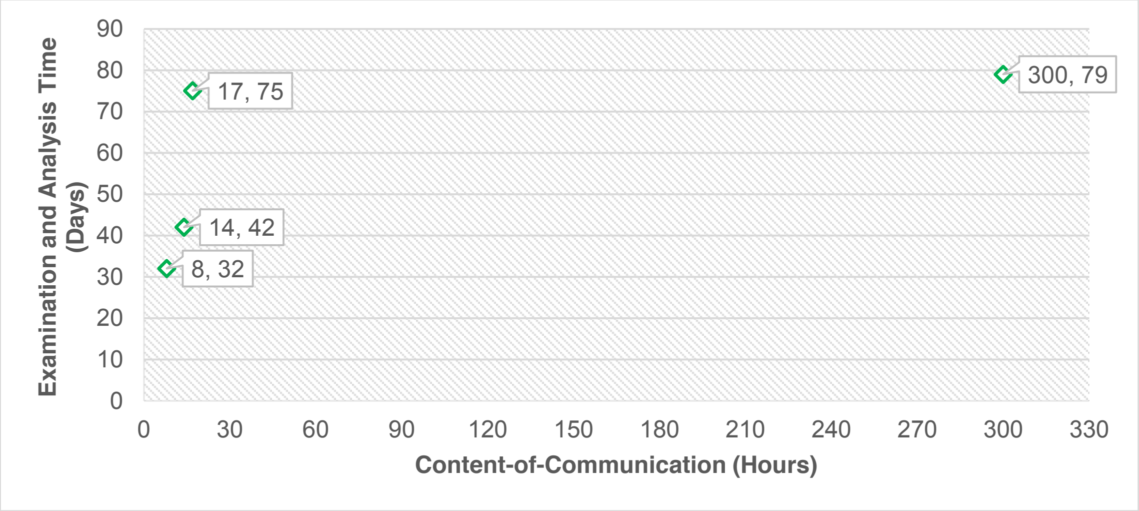


Figure 23. The hours of content-of-communication and the examination and analysis time.

Table 29. *Hours of Content-of-communication and the Examination and Analysis Time – **Correlation**.*

| | | Examination and Analysis Time | Hours of Content-of-communication |
|---|---|---|---|
| Examination and Analysis Time | Pearson Correlation | 1 | .642 |
| | Sig. (2-tailed) | | .358 |
| | N | 4 | 4 |
| Hours of Content-of-communication | Pearson Correlation | .642 | 1 |
| | Sig. (2-tailed) | .358 | |
| | N | 4 | 7 |

### 4.3.5.3. Mobile Network Data Volume and the Juristic Processing Time

#### 4.3.5.3.1. Localization Data

Figure 24 shows the number of localization data records on the x-axis and the juristic processing time on the y-axis. The corresponding correlational table is displayed in Table 30, *r* = .594, p > .05. In contrast to the forensic processing, the juristic processing time is in a positive correlation with the number of localization records, although not statistically significant due to the small number of cases considered.

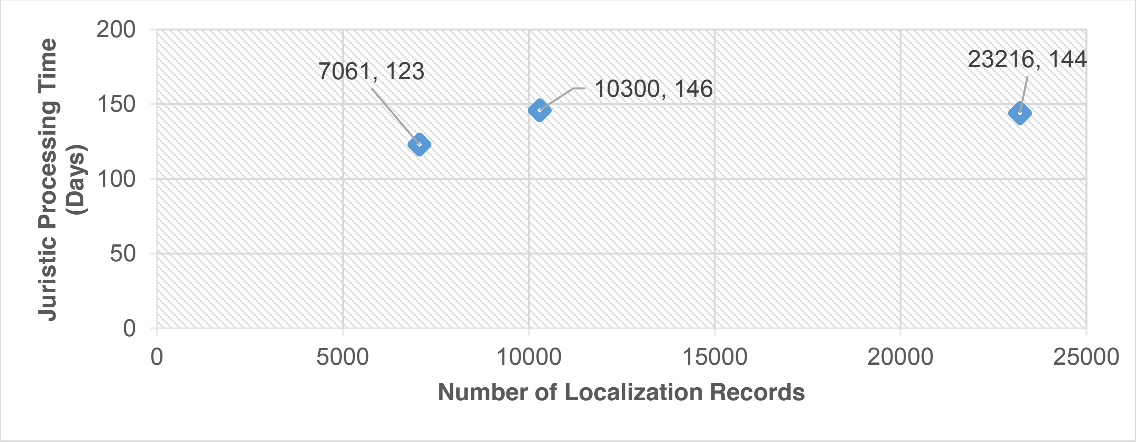


Figure 24. The number of localization records and the juristic processing time.

Table 30. *Number of Localization Data Records and the Juristic Processing Time – **Correlation***.

| | | Juristic Processing Time | No. of Localization Records |
|---|---|---|---|
| Juristic Processing Time | Pearson Correlation | 1 | .594 |
| | Sig. (2-tailed) | | .595 |
| | N | 3 | 3 |
| No. of Localization Records | Pearson Correlation | .594 | 1 |
| | Sig. (2-tailed) | .595 | |
| | N | 3 | 7 |

4.3.5.3.2. Network-management Data

Figure 25 shows the number of network-management data records on the x-axis and the juristic processing time on the y-axis. The corresponding correlational table is displayed in Table 31, $r$ = -.983, p < .05 (p=0.017). The statistically significant Pearson's coefficient suggests that the network-management data affect the juristic decision-making, enabling faster courtroom case processing with a larger number of network-management records.

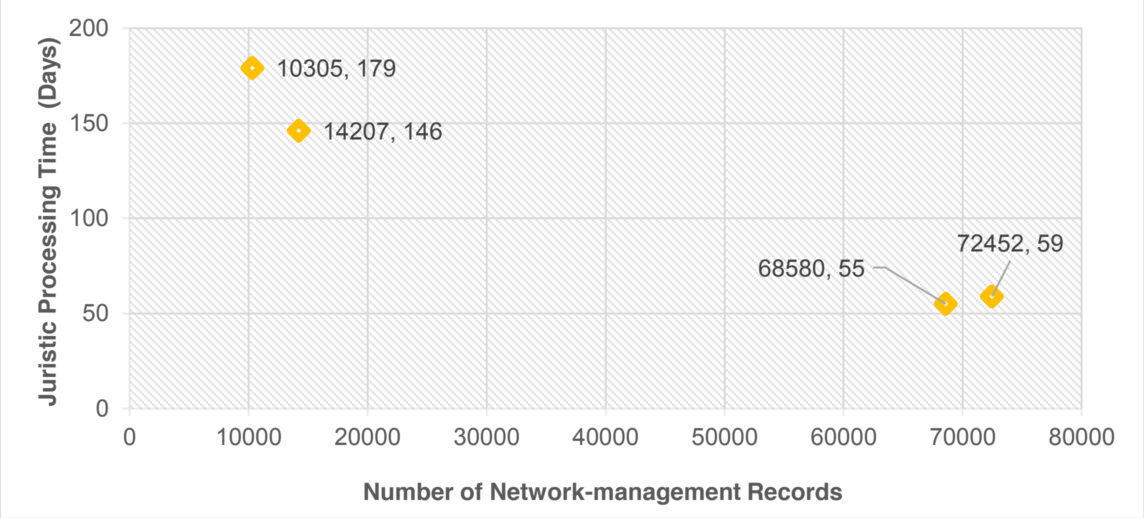


Figure 25. The number of network-management records and the juristic processing time.

Table 31. *Number of Network-management Data Records and the Juristic Processing Time –* ***Correlation****.*

| | | Juristic Processing Time | No. of Network-management Records |
|---|---|---|---|
| Juristic Processing Time | Pearson Correlation | 1 | -.983* |
| | Sig. (2-tailed) | | .017 |
| | N | 4 | 4 |
| No. of Network-management Records | Pearson Correlation | -.983* | 1 |
| | Sig. (2-tailed) | .017 | |
| | N | 4 | 7 |

*. Correlation is significant at the 0.05 level (2-tailed).

### 4.3.5.3.3. Content-of-communication Data

Figure 26 shows the number of content-of-communication hours on the x-axis and the juristic processing time on the y-axis. The corresponding correlational table is displayed in Table 32, *r* = .988, p < .05 (p = 0.012). The statistically significant Pearson's coefficient suggests that the content-of-communication data affect the juristic decision-making, extending the courtroom case processing the hours of content-of-communication presented as evidence.

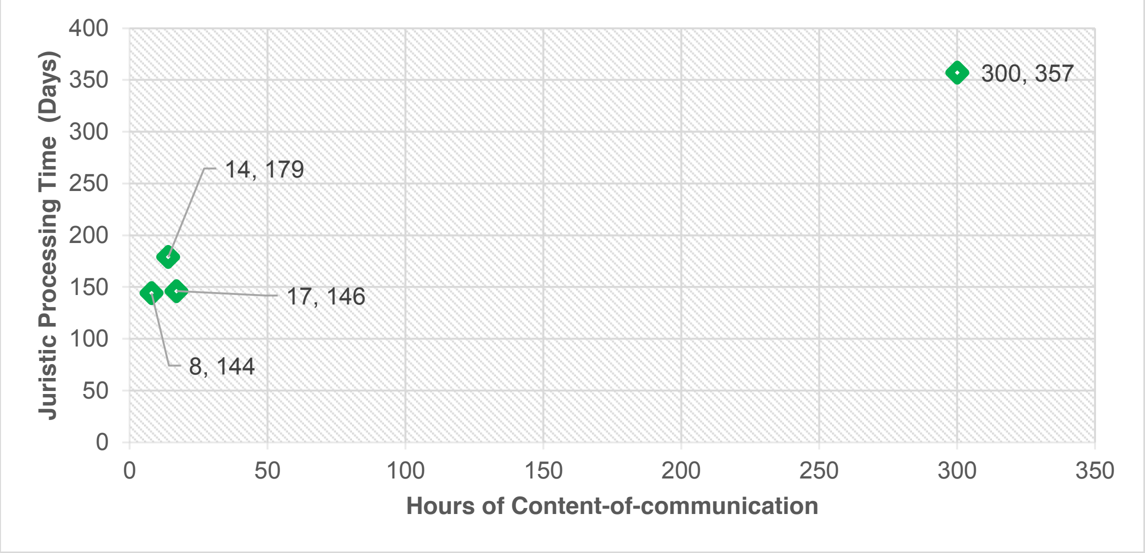


Figure 26. The hours of content-of-communication data and the juristic processing time.

Table 32. *Hours of Content-of-communication and the Juristic Processing Time –* ***Correlation*****.**

| | | Juristic Processing Time | Hours of Content-of-communication |
|---|---|---|---|
| Juristic Processing Time | Pearson Correlation | 1 | .988$^{*}$ |
| | Sig. (2-tailed) | | .012 |
| | N | 4 | 4 |
| Hours of Content-of-communication | Pearson Correlation | .988$^{*}$ | 1 |
| | Sig. (2-tailed) | .012 | |
| | N | 4 | 7 |

*. Correlation is significant at the 0.05 level (2-tailed).

#### 4.3.5.4. Mobile Network Data Volume and the Case Disposition Time

##### 4.3.5.4.1. Localization Data

Figure 27 shows the number of localization data records on the x-axis and the juristic processing time on the y-axis is depicted in presented 27. The corresponding correlational table is displayed in Table 33, *r* = -.274, p > .05. Analogously to the juristic processing time, the overall case disposition time is negatively correlated with the number of localization records, considering the statistical insignificance.

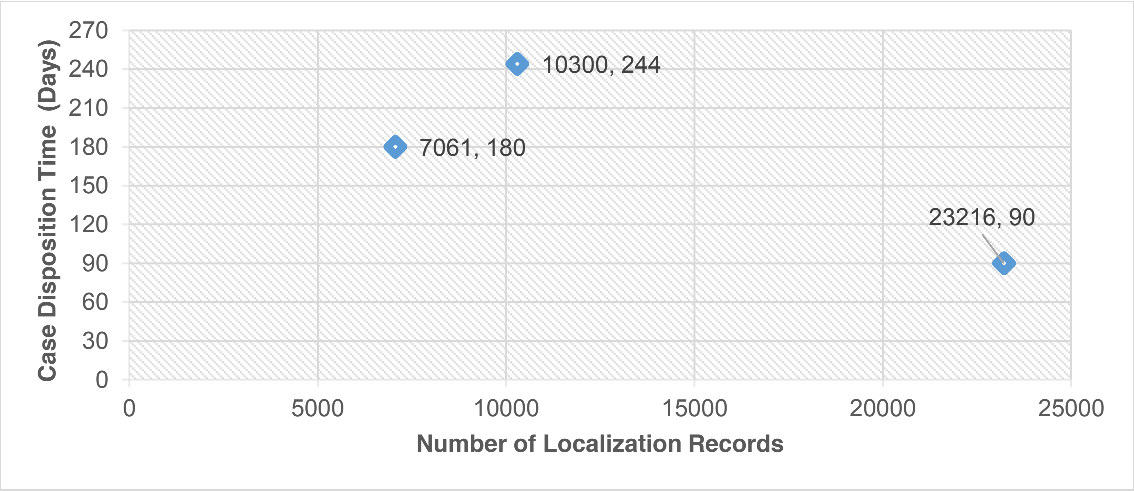


Figure 27. The number of localization records and the case disposition time.

Table 33. *Number of Localization Data Records and the Case Disposition Time –* ***Correlation***.

| | | Case Disposition Time | No. of Localization Records |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | -.274 |
| | Sig. (2-tailed) | | .824 |
| | N | 3 | 3 |
| No. of Localization Records | Pearson Correlation | -.274 | 1 |
| | Sig. (2-tailed) | .824 | |
| | N | 3 | 7 |

4.3.5.4.2. Network-management Data

Figure 28 shows the number of network-management data records on the x-axis and the case disposition time on the y-axis. The corresponding correlational table is displayed in Table 34, *r* = -.985, p < .05 (p=0.015). The statistically significant Pearson's coefficient suggests that the network-management data are negatively correlated with the case disposition time.

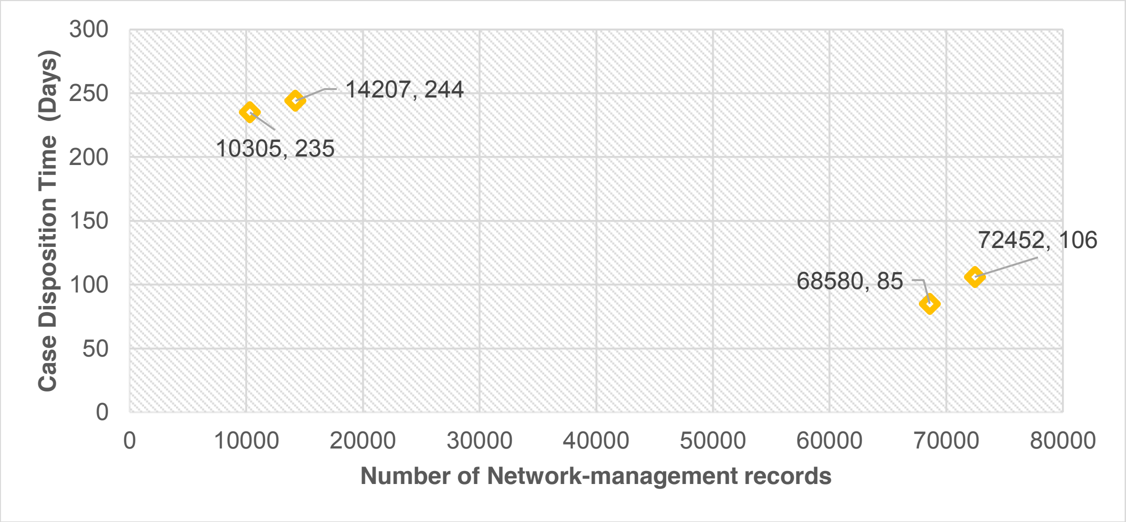


Figure 28. The number of network-management records and the case disposition time.

Table 34. *Number of Network-management Data Records and the Case Disposition Time – **Correlation**.*

| | | Case Disposition Time | No. of Network-management Records |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | -.985* |
| | Sig. (2-tailed) | | .015 |
| | N | 4 | 4 |
| No. of Network-management Records | Pearson Correlation | -.985* | 1 |
| | Sig. (2-tailed) | .015 | |
| | N | 4 | 7 |

*. Correlation is significant at the 0.05 level (2-tailed).

4.3.5.4.3. Content-of-communication Data

Figure 29 shows the number of content-of-communication hours on the x-axis and the juristic processing time on the y-axis is depicted in Figure 29. The corresponding correlational table is presented in Table 35, *r* = .978, p < .05 (p = 0.022). The statistically significant Pearson's coefficient suggests that the content-of-communication data are positively correlated with the case disposition time.

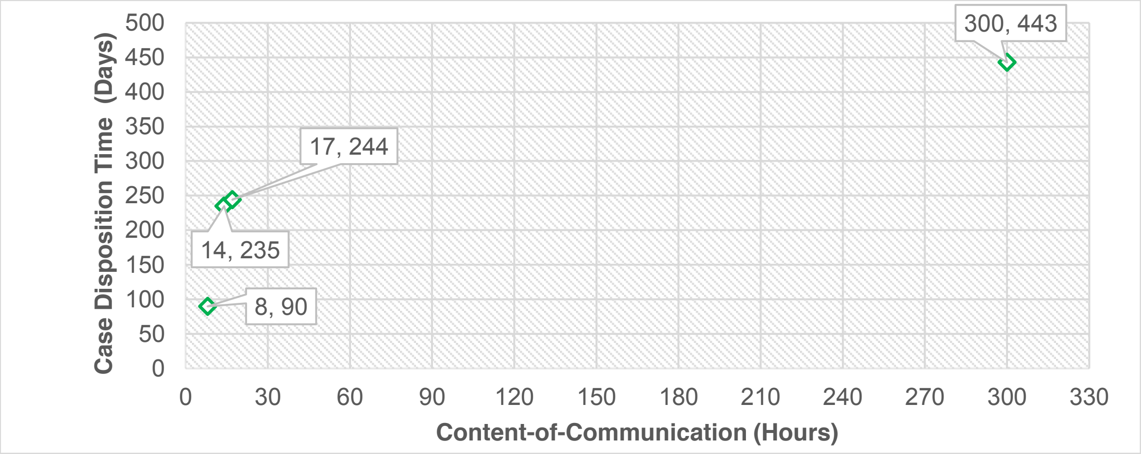


Figure 29. The hours of content-of-communication data and the case disposition time.

Table 35. *Hours of Content-of-communication and the Case Disposition Time –* ***Correlation***.

| | | Case Disposition Time | Hours of Content-of-communication |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | .978* |
| | Sig. (2-tailed) | | .022 |
| | N | 4 | 4 |
| Hours of Content-of-communication | Pearson Correlation | .978* | 1 |
| | Sig. (2-tailed) | .022 | |
| | N | 4 | 7 |

*. Correlation is significant at the 0.05 level (2-tailed).

4.3.5.5. Mobile Network Data Volume and the Case Processing Performance – Summary

Table 36 summarizes the Pearson's correlation coefficients for each of the mobile network data types and the forensic and juristic processing times.

Table 36. *Mobile Network Data Volume – **Pearson's Correlation Coefficient Summary***.

| | Acquisition and Delivery Time | Examination and Analysis Time | Juristic Processing Time | Case Disposition Time |
|---|---|---|---|---|
| Localization data | -.969 | -.385 | .594 | -.274 |
| Network-management data | -.195 | -.803 | -.983* | -.985* |
| Content-of-communication data | -.523 | .642 | .988* | .978* |

*. Correlation is significant at the 0.05 level (2-tailed).

Overall, the mobile network volume was not found to have any effect on the acquisition and delivery time. However, the first column in Table 36 indicates a negative correlation between the volume and the acquisition and delivery time for all the mobile network data types. As noted in the analysis of the relationship between the mobile network data variety and the acquisition and delivery time in section 4.3.4.1, there might be other factors with a confounding effect on the acquisition and delivery process that mask the impact of the mobile network data volume on the time needed to be brought in forensic custody (section 4.4 discusses the acquisition and delivery process from an institutional perspective to reveal these factors).

Similarly, the mobile network volume was not found to have any effect on the examination and analysis time. A closer look at the second column of Table 36 reveals a negative correlation between the volume and the examination and analysis for the non-real time data (localization and network-management data), but positive correlation for the real-time data (content-of-communication). As noted in the analysis of the relationship between the mobile network data variety and the examination and analysis time in section 4.3.4.2, there might be other factors with a confounding effect on the forensic examination and analysis that mask the impact of the mobile network data volume on the time need to be forensically processed (section 4.4 discusses the forensic evidence production process from an institutional perspective to reveal these factors).

While the mobile data volume is not a significant factor that affects the forensic processing in general, the third and the fourth columns in Table 36 indicate that the number of network-management records and the hours of content-of-communication data do in fact impact the juristic processing, and with that, the overall case disposition. For the network-management data, a negative correlation is characteristic for every phase of the case processing process, culminating with a significantly strong relationship with the overall case disposition. For the content-of-communication data, the negative correlation in acquisition phase was reverted in the phase when this data types was forensically processed, achieving a statistically significant positive correlation in the juristic processing phase and the overall case disposition. This outcome indicates that the both the forensic and juristic processing of these data types is dependent on their innate probative value and relevance as evidentiary element for the criminal hypothesis testing.

### 4.3.6. Forensic Processing Contribution

#### 4.3.6.1. Acquisition and Delivery Time and the Case Disposition Time

Figure 30 shows the acquisition and delivery times on the x-axis and the case disposition time on the y-axis for each of the cases in the sample. The corresponding correlational table is displayed in Table 37, *r* = -.317, p > .05. The statistically insignificant correlation prevents formal generalization of the relationship between the acquisition and delivery time and the case disposition time.

Accounting for the negative correlational coefficient too, the analysis was repeated without the outlier Case III, showing the relationship on Figure 31 and the corresponding correlational table in Table 38, r=.241, p > 0.05. This change has not affected the statistical significance, however, it reverted the correlation trend to a positive one. Given that the case disposition time aggregates the acquisition and delivery time, the positive correlation aligns with the intuitive expectation of a positive correlation. .

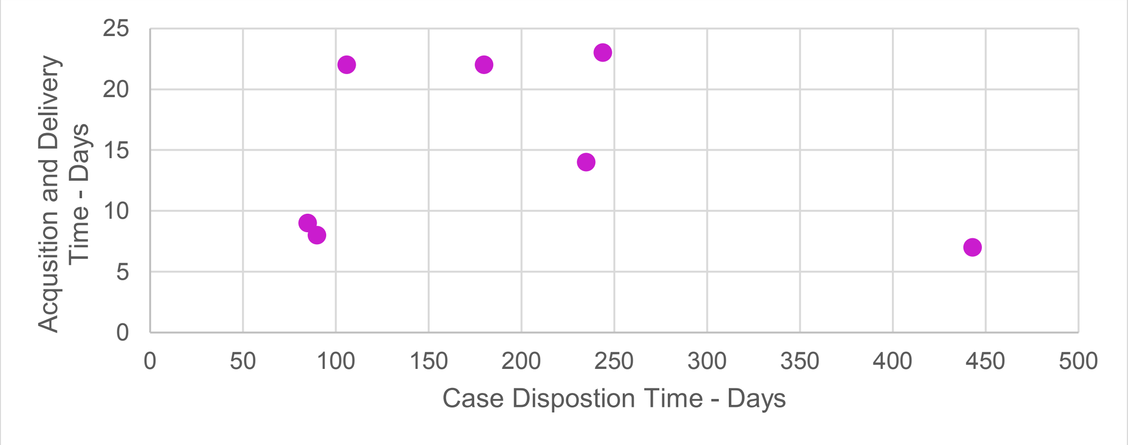


Figure 30. The acquisition and delivery time and the case disposition time.

Table 37. *Acquisition and Delivery Time and the Case Disposition Time – **Correlation***.

| | | Case Disposition Time | Acquisition and Delivery Time |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | -.317 |
| | Sig. (2-tailed) | | .489 |
| | N | 7 | 7 |
| Acquisition and Delivery Time | Pearson Correlation | -.317 | 1 |
| | Sig. (2-tailed) | .489 | |
| | N | 7 | 7 |

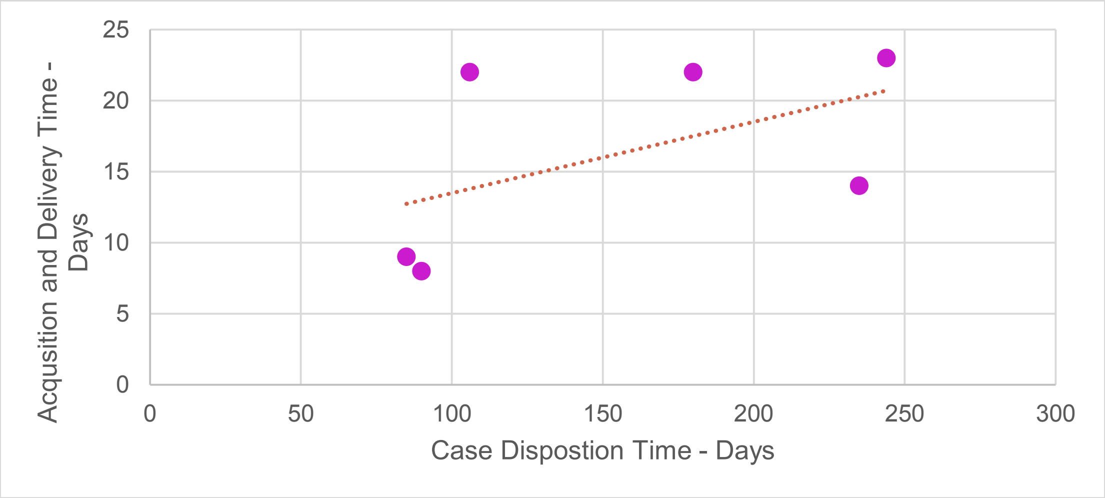


Figure 31. The acquisition and delivery time and the case disposition time, without the outlier Case III.

Table 38. *Acquisition and Delivery Time and the Case Disposition Time*, without the outlier Case III – ***Correlation***.

| | | Case Disposition Time | Acquisition and Delivery Time |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | .241 |
| | Sig. (2-tailed) | | .645 |
| | N | 6 | 6 |
| Acquisition and Delivery Time | Pearson Correlation | .241 | 1 |
| | Sig. (2-tailed) | .645 | |
| | N | 6 | 6 |

4.3.6.2. Examination and Analysis Time and the Case Disposition Time

Figure 32 shows the examination and analysis time on the x-axis and the case disposition time on the y-axis for each of the cases in the sample. The corresponding correlational table is displayed in Table 39, $r = .875$, $p < .05$ ($p = 0.01$). The statistically significant positive correlation suggests that the cases are disposed in correlation with the time needed for the mobile data to be forensically processed. Next to the volume and the variety aspects, the structure of each data type is relevant here, because the examination and analysis procedures and the application in the criminal hypothesis testing differs whether localization, network-management, or content-of-communication data are used (section 4.4 includes a discussion on this relationship)

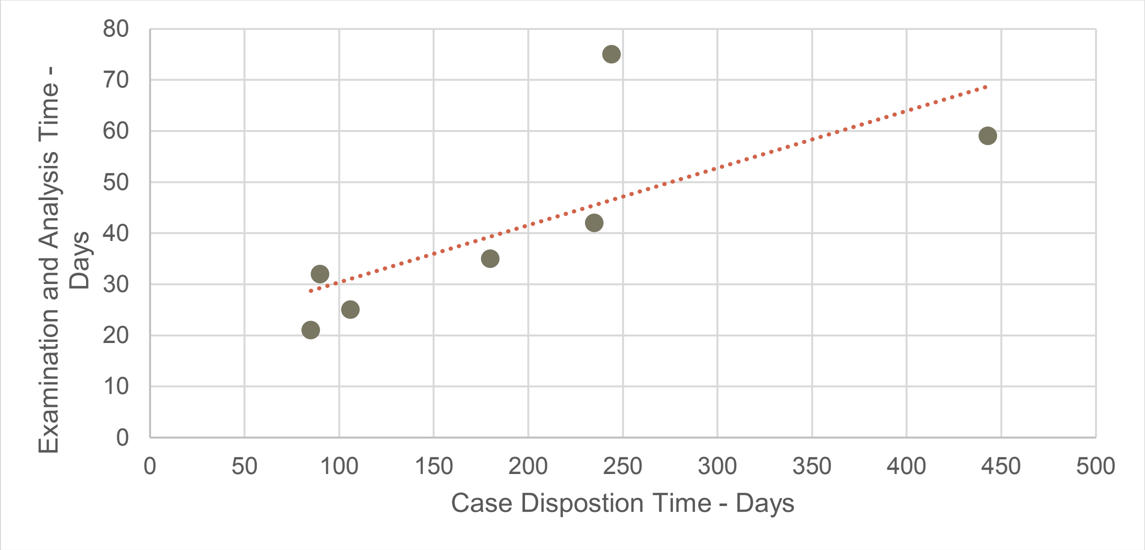


Figure 32. The examination and analysis time and the case disposition time.

Table 39. *Examination and Analysis Time and the Case Disposition Time –* ***Correlation***.

| | | Case Disposition Time | Examination and Analysis Time |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | .875** |
| | Sig. (2-tailed) | | .010 |
| | N | 7 | 7 |
| Examination and Analysis Time | Pearson Correlation | .875** | 1 |
| | Sig. (2-tailed) | .010 | |
| | N | 7 | 7 |

**. Correlation is significant at the 0.05 level (2-tailed).

4.3.6.3. Juristic Processing Time and the Case Disposition Time

Figure 33 shows the juristic processing times on the x-axis and the case disposition time on the y-axis for each of the cases in the sample. The corresponding correlational table is displayed in Table 40, $r$ = .987, p < .05. The statistical significance of the correlation is expected in this case (p =0.001), given that the juristic processing effort is what brings the case to an end, or in other words, it actualizes the case disposition.

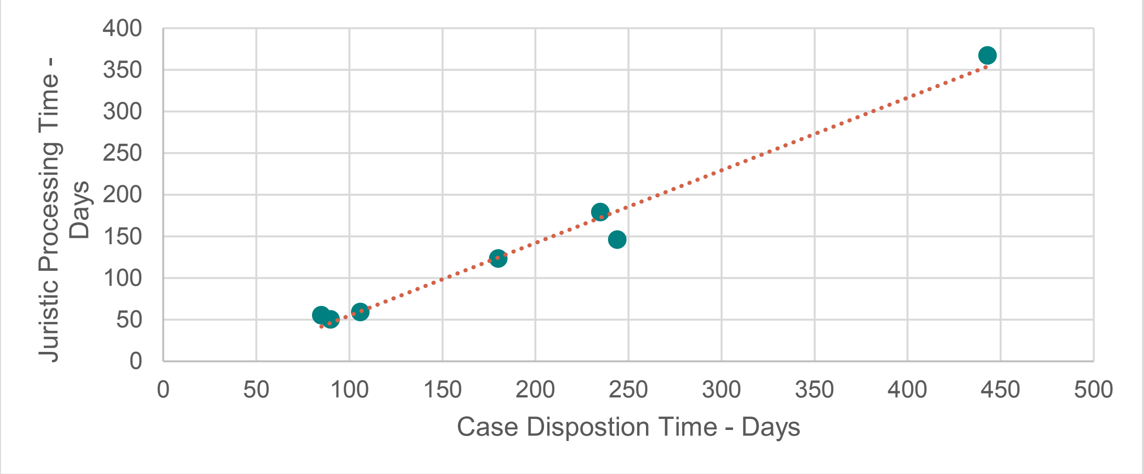


Figure 33. The examination and analysis time and the case disposition time.

Table 40. *Juristic Processing Time and the Case Disposition Time – **Correlation**.*

| | | Case Disposition Time | Juristic Processing Time |
|---|---|---|---|
| Case Disposition Time | Pearson Correlation | 1 | .987** |
| | Sig. (2-tailed) | | .000 |
| | N | 7 | 7 |
| Juristic Processing Time | Pearson Correlation | .987** | 1 |
| | Sig. (2-tailed) | .000 | |
| | N | 7 | 7 |

**. Correlation is significant at the 0.05 level (2-tailed).

4.3.6.4. Forensic processing contribution in the case processing performance – Summary

Table 41 summarizes the Pearson's correlation coefficients for each case processing phases and the overall case disposition time.

Table 41. *Forensic Processing Contribution –* ***Pearson's Correlation Coefficient Summary***.

| | Case Disposition Time |
|---|---|
| Acquisition and Delivery Time | .241 |
| Examination and Analysis Time | .875* |
| Juristic Processing Time | .987* |

*. Correlation is significant at the 0.05 level (2-tailed).

The positive correlation trend is intuitively expected, given that the case disposition time aggregates the time spent in each of these phases. Abstracting both the variety and volume aspects of the mobile network data, it follows that forensic processing contributes significantly to the case processing performance given that the examination and analysis effort is strictly devoted in extracting and interpreting the associated probative value. The significance of the strong correlation for the juristic processing time corroborates the observation on the mobile network data relevancy-based contribution, following that once it is introduced as an evidence in courtroom, the mobile network data becomes an indisputable argument in the judicial decision-making.

## 4.4. Content Analysis

The content analysis takes a closer look at the case data information – or what is referred as the exploratory matrix in section 3.2.1 - to reveal the impact of the confounding factors on the acquisition and delivery process, the examination and analysis process, and the juristic process of criminal justice delivery.

### 4.4.1. Confounding Factors – Impact on the Forensic Processing

The confounding factors with an impact on the acquisition and delivery time and the examination and analysis time include:

- the set of actors involved when different data types are retrieved
- the number of target identities
- the investigation timespan (the period for which the mobile network activity of these target identities is needed)
- the delivery formats, and
- the forensic processing methodologies

#### 4.4.1.1.Evidence Acquisition and Delivery Procedure – Actors, Target Identities, and Investigation timespan

The acquisition and delivery procedure involves different set of actors for the non-real time mobile network data types versus for the real time data type as depicted in Table 42. The prosecution collects the localization and the network-management records by sending a request including the target identities investigated and the investigation timespan directly to the mobile operators (the network-management data from other visiting operators in Case VIII was requested through the Ministry of Justice liaisons). For the content-of-communication data, the prosecution requests an interception of the target identities' communication from the NLEA for a specific investigation timespan in each of the cases.

The legislative framework in Macedonia permits content-of-communication acquisition and delivery only by the NLEA with a previously established authorization and data handover protocol. The purpose is to ensure secure transfer of the intercepted audio material and privacy protection of the target identities, for which actual proofs were provided in each of the case reports. Here it must be noted that the legislative framework does not prescribe implementation of the recommended 3GPP interfaces for lawful interception and evidence retrieval between each of the actors involved. Therefore, the case reports have not indicated that the mutual authentication and authorization between the prosecution and the operators (Ministry of Justice liaisons) and NLEA was executed over the 3GPP-recommended HI1 interface. Also, no information was found whether the localization and network-management data were delivered over the 3GPP-recommended HI2 interface, or the content-of-communication data over the HI3 interface.

Table 42. *Evidence Acquisition and Delivery Procedure - Actors*

| Actors | Non-real time data (localization and network-management data) | Real time data (content-of-communication) |
|---|---|---|
| Prosecution | ✓ | ✓ |
| Mobile Operators | ✓ | ✗ |
| Ministry of Justice Liaisons* | ✓ | ✗ |
| NLEA | ✗ | ✓ |

*only for the network-management data retrieved from multiple jurisdictions

Back to the research question, localization data, network-management data and the content-of-communication data affect the acquisition and delivery segment of the case processing process by the time needed each operator or the NLEA to respond to the prosecution request. In addition, the acquisition and delivery time is also affected by the time needed the non-real time data and the real-time data to be acquired and combined before they are forensically processed for the medium and maximum variety cases.

The response time is determined by the number of times the operators and/or the NLEA need to invoke their internal data collection procedures, the volume of the mobile network data, and the immediate availability of the data. For each target identity, these collection procedures are invoked at least once for each of the mobile network data types for the investigation timespan requested (if the non-real time data are not immediately available, further collection is needed from the internal operators' storage). The investigation timespan, on the other hand, yields different data volume depending on the target identities' mobile service usage, which requires different time to be collected.

The number of target identities and the investigation timespan shown in Figure 34(a) and Figure 34(b) are therefore pointed as confounding factor that impact the time needed for the mobile network data volume to be aggregated and delivered back to the prosecution by either the operators or the NLEA. Given that for the medium and maximum variety cases, the prosecution needs to collect data from more than one source, the actors are also pointed out as a confounding factor because they use different collection procedures that depend on the data type structure (that is, the localization and network-management data are collected from the internal databases on operators side, while the content-of-communication data are captured from the communication stream passing the mobile infrastructure). The difference in collection procedures can yield different response times, which in turn, requires the prosecution to wait until all data are delivered before it combines them and sends for forensic processing. Therefore, the actors involved are identified as a confounding factor next to the target identities and the investigation timespan in the acquisition and delivery segment of the case processing process.

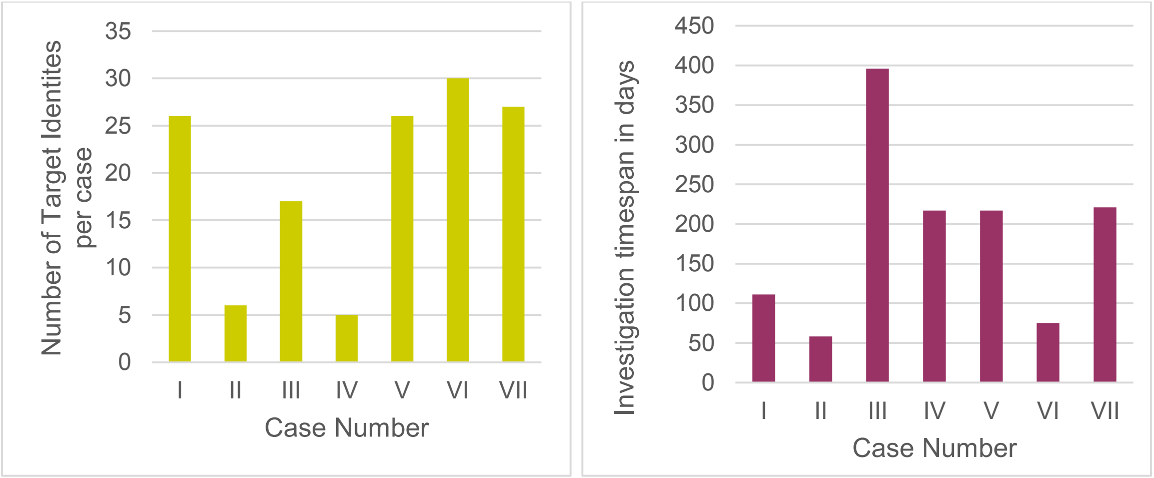


Figure 34. The remaining case information from the case reports for each case in the sample. (a) Number of target identities investigated. (b) Investigation timespan in days.

#### 4.4.1.2.Forensic Handling Procedure – delivery formats and forensic processing methodologies

The localization data, network-management data and the content-of-communication data affect the examination and analysis segment of the case processing process by the time needed to be examined, analyzed and interpreted as of associated criminal events for each target identity. In addition, the examination and analysis time is also affected by the time needed the non-real time data and the real-time data to be consolidated per target identity for the medium and maximum variety cases. The objective of the forensic processing for each of the mobile network data is:

- For the localization data, the objective is to reconstruct the movement pattern based on the event date/time/*Origin MSISDN* and the *longitude* and *latitude* attributes. This requires data sorting and geolocation map rendering.
- For the network-management data, the objective is to reconstruct the service behavior based on the *Event Date/Time/Duration*, *Observed MSISDN* and the *Connected Number* attributes. This requires data sorting, aggregating, grouping, interlinking and data joining for each of the target identities (MSISDNs)

  For the content-of-communication data, the objective is to single out the critical conversation portions relevant to the criminal hypothesis based on the *Event Date/Time/Duration*, *Observed MSISDN* and *Connected Number* attributes. This requires replying of the intercepted conversations (for several times) to capture the critical conversational part of the audio data, extract the timestamp and sort/interlink with the information for each of the target identity (MSISDNs) investigated.

For the localization data, all the operators have included only the *longitude* and *latitude* attributes associated with the position of the target identity, although the *3GPP positioning protocol* prescribes reporting of the *altitude*, *altitude direction*, *uncertainty minor/major ellipsoid*, and *confidence* attributes for precise positioning (3rd Generation Partnership Project, 2015b). For the network-management data, not all operators have included the *Observed IMSI* attribute and all of them omitted the *Correlation Number* attribute. For the content-of-communication data, NLEA has omitted both the *Lawful Interception Identifier* and the *Correlation Number* attributes.

The case data show that instead of using this number, the mobile network data were correlated on the *Event Date/Time/Duration*, *Observed MSISDN* and *Observed IMEI* attributes. This is not in alignment with the prescribed ISO/IEC 27042 methodology for probative value extraction, which according to the forensic reports was employed in processing the mobile network data in each case together with the ISO/IEC 27035:2011 measures for privacy and integrity protection.

The inconsistence in the evidence delivery formats as a confounding factor impacts the time needed the mobile data to be examined, analyzed and interpreted in that it requires additional time to be invested in checking the precision of the localization coordinates and in consolidating the non-real time data and real time data for each of the target identity on multiple attributes instead of one, that being the *Correlational Number* attribute. The non-compliance in the forensic processing methodologies is also included as a confounding factor because by using a proprietary approach for probative value extraction the consolidation can consume different examination and analysis time depending on which operator has delivered the data (the *Observed IMSI* attribute was not included by all operators, therefore the forensic practitioners might need different times in using the remaining attributes for those records in the consolidation process).

### 4.4.2. Confounding Factors – Impact on the Case Processing

The confounding factors with an impact on the juristic processing time and the overall case disposition time include:

- the degree of certainty associated with each mobile data type
- the criminal offense processed

The localization data, network-management data and the content-of-communication data affect the juristic processing segment and the overall case processing process by the degree of probative value they bring in the courtroom reconstruction of the criminal activities:

- *Localization data* - the movement pattern is used to establish the point of present of each of the target identities for a given date, time and location of interest during the investigation timespan.
- *Network-management data* - the service behavior profile is used to establish the connection between each of the target identities investigated within the investigation timespan. It is also used to check the trustworthiness of the criminal behavior profile developed using the remaining evidence in the case (Ayers et al., 2014; Forte & Donno, 2010).
- Content-of-communication data - the critical conversation portions are used to support the criminal events reconstruction as of the interaction exchanged between the target identities during the investigation timespan.

Next to the volume and variety, the probative value is also affected by the degree of certainty associated with each mobile data type. That is, the extent to which the mobile network data is conclusive for a given criminal event. For the localization data, there is a small degree of uncertainty associated with the precision on the longitude and latitude coordinates (Blank, 2011; O'Malley, 2011; Wells, 2014). Because the 3GPP positioning protocol in the localization record format specified only the *longitude* and l*atitude* associated with the position of the target identity, but not attributes giving the *altitude*, *altitude direction*, *uncertainty minor*/*major ellipsoid*, and *confidence* (3rd Generation

Partnership Project, 2015b), there might be a potential discrepancy in the actual position of the target identity and the one registered by the 3GPP-compliant network.

No uncertainty is associated with the network-management data because they represent the interactions carried over a 3GPP-compliant network that certainly occurred, being initiated by or directed to the target identity of interest. Another argument for their high conclusiveness is their primary purpose and critical importance for the normal operation of the mobile operators (network, maintenance, optimization, billing…).

No uncertainty is associated with the content-of-communication data too, because they represent the actual conversations carried over the 3GPP-compliant network between the investigated target identities. Another argument for their high conclusiveness is that they are in fact the actual copies of the conversation(s) that took place between two or more target identities, which can be mutually verified for every conversation.

The degree of certainty associated with each mobile data type is included as a confounding factor to the juristic processing and the overall case processing because the judges rest their decision-making on their confidence in the probative value of the mobile network data. That is, next to the volume and variety aspects, the probative value – or the relevance of the mobile network data to the criminal hypothesis testing – is also taken as an argument in rendering the verdict and brining the pending case to an end.

The probative value of the mobile network data in the criminal hypothesis testing is affected by the type of criminal offense processed in case. To this point, Table 43 enlists the criminal offenses processed in each of the sample cases, categorized according to the Criminal Code of Macedonia and the International Crime Classification System (Assembly of the Republic of Macedonia, 2013; UNODC & UNECE, 2012).

Table 43. *Criminal Offenses Processed in Each Case*

| Case Sample | Criminal Offence |
|---|---|
| Case I | Dealing narcotics, psychotropic substances and precursors |
| Case II | Unlawful possession of weapons or explosive materials |
| Case III | Money laundering and tax evasion |
| Case IV | Unauthorized production and release for trade of narcotics, psychotropic substances, and precursors |
| Case V | Human trafficking |
| Case VI | Founding a slave relationship and transportation of persons in slavery |
| Case VII | Unlawful property gain and money laundering |

For Case I, the prosecution requested the localization data to yield the points of presence and the movement patterns of the perpetrators with the witnessing/investigating parties, given the charges of dealing narcotics. For Case II the network-management data were requested to yield the date/time and the numbers to which the suspects have communicated during the investigative period as to test prosecution's hypothesis on the unlawful possession of weapons.  For Case III, the content-of-communication data were brought as an evidence yielding the coordination, preparation, execution, and the hierarchy of the overall money laundering and tax evasion scheme.

For Case IV, the prosecution requested content-of-communication data together with network-management data to reveal the service behavior and the conversational details on how the suspects organized and realized the drug production. For Case V, the prosecution requested content-of-communication data together with the localization data to reconstruct the human trafficking movement trace. For Case VI, the prosecution combined all three mobile network data types to evidence the subjugation of the victims (threatening calls, coordination), and to chronologically and geographically reconstruct the trafficking channel between the southern and the northern borders of Macedonia. For Case VII, the unlawful property gain and money laundering criminal offence spanned across several jurisdictions, therefore, the prosecution requested network-management data both from the local operators and six other visiting operators to reconstruct the organized crime scheme.

The criminal offense type is included as a confounding factor to the juristic processing and the overall case processing because the case overall is disposed not just on the mobile network data alone, but also using the remaining evidence and courtroom testimonials. That is, next to the volume, variety, and the probative value aspects, the verdict that brings the pending case to an end encompasses juristic syllogism that next to the mobile network data includes additional information with pertinence to the criminal offense processed.

### 4.4.3. Confounding Factors – Impact on the Relationship between the Forensic and Case Processing

The confounding factor with an impact on the relationship between the forensic processing times and the case processing times refers to the internal structure of each of the mobile network data types. As noted in section 4.4.2, the structure of the localization data imply data sorting and geolocation map rendering during the examination and analysis time for the probative value to be extracted per each target identity.

Analogously, the structure of the network-management data imply data sorting, aggregating, grouping, interlinking and data joining, and the structure of the content-of-communication data imply replay of the intercepted conversations. In the context of the examination and analysis time, this translates into additional time needed for the cases that include more than one data type because each data type first needs to be examined separately and then consolidated with the other (two) data types per each target identity. On a similar account, the extracted movement behavior and service usage behavior imply graphical presentation while the conversational interactions imply audio presentation in courtroom, which in turn requires more courtroom time when the cases including content-of-communication are juristically processed.

The structure of the mobile network data type is therefore set as a confounding factor because next to the forensic skills and methodologies and the degree of certainty associated with each mobile data type, the relationship between the forensic processing and case processing is also contingent on the basic properties each data type incorporates. Essentially, the nature of the mobile network data frames the basic approach in its processing – being that either forensic or juristic – and with the overall execution time for a criminal case to be disposed.

### 4.4.4. Content Analysis Summary

The content analysis revealed the potential factors influencing the relationships analyzed in section 4.3 by coupling the exploratory matrix information together with the research variables data. The set of evidence delivery actors, the number of target identities, the investigation timespan, the delivery formats, and the forensic processing methodologies are identified as the confounding factors with an impact on forensic processing times, next to the mobile network data volume and variety. The degree of certainty associated with each mobile data type and the criminal offense processed were identified as the confounding factors with an impact on the juristic processing time and the overall case disposition time. The basic structural properties of the mobile network data were identified as the factor that affects the relationship between the forensic and case processing times.

The following chapter approaches overall analytical output from an institutional perspective to render the contribution of the mobile network data in the case processing performance , as well as the implications for actions in the current practice and future research.

# 5. DISCUSSION, CONCLUSIONS, IMPLICATIONS FOR ACTION

This chapter presents the discussion, conclusions, and the implications for actions derived from this study. The results from the statistical analysis are coupled with the output of the content analysis under the IAD framework in discussing the mobile network data contribution in the criminal case processing in Macedonia. The conclusions drawn are then furthered to discuss the implications for the case processing practice in Macedonia, as well as the implications for the future research.

## 5.1. Mobile Network Data Variety Contribution – Discussion

### 5.1.1. Acquisition and Delivery Segment

The larger acquisition and delivery time for cases with two mobile network data types compared with the cases including only one data type as evidence is a logical result, considering Table 42 from section 4.4.1. One reason for this outcome is the lack of legal compulsion regulating the evidence delivery coordination between the operators and the NLEA. Without a coordinated evidence collection and no time limits imposed on responding back to the prosecution, it is reasonable to expect fluctuations in the acquisition and delivery time. The number of target identities involved and the investigation timespan also plays a role here, given that the operators and the NLEA determine the time of their response as of the number of times they need to invoke their internal data collection procedures and the immediate availability of the data.

Another reason might be the non-3GPP compliant evidence acquisition and delivery procedure. Given that the use of the recommended 3GPP interfaces implies coordination for all actions when collecting different data types, the lack thereof leaves the acquisition and delivery time to fluctuate on case-to-case basis as of the number of mobile network data types included as evidence.

### 5.1.2. Examination and Analysis Segment

The statistically insignificant relationship between the mobile network data variety and examination and analysis time might be explained by a confounding effect of the mobile network data volume, given that the examination and analysis phase actually is a fact finding process equally affected by both the mobile data variety and volume, as well as the common denominator linking them, that is, the target identities investigated (the MSISDNs/IMEIs/IMSIs). The statistical significance of the ANOVA output – without the maximum (extreme) volume case of content-of-communication data (Case III) – is an expected outcome, given that the forensic processing for each of the mobile network data type requires a different approach, based on their relevance to the criminal hypothesis, as pointed in section 4.1.1.2

The different approaches translate into different times need for the mobile network data to be processed, and even more, to be consolidated based on data structure and the number of target identities investigated. Recalling that the localization data were not strictly formatted as of the 3GPP positioning protocol, the forensic processing needed further time to verify the movement pattern reliability by manual, record-by-record checks. The same holds true in the case when the non-real time data are consolidated with the content-of-communication data. The omission of the *Correlation Number* incurs additional forensic processing time because the records must be correlated manually by the *Event Date/Time/Duration*, *Observed MSISDN* and/or the *Observed IMEI* attribute for each target identity. Therefore the fluctuations in the examination and analysis time caused by the mobile network data variety are logical consequence of the deviation from the recommended 3GPP and ISO/IEC SC 27 compliance as noted in section 4.4.2.

The foregoing discussion also holds for the interesting difference in the forensic processing for the cases where the localization and network-management data are included separately, and when they are combined with the content-of-communication. That is, it is reasonable to expect a prolongation of the examination and analysis time for the cases with content-of-communication data, having the forensics effort doubled in the later instance – once to develop the movement pattern or the service behavior profile, and once to select the critical conversational parts and consolidate them with these profiles for each of the target identities investigated.

### 5.1.3. Juristic Processing and Case Disposition Segment

The statistically insignificant relationship of the juristic processing in respect the mobile data variety is an expected outcome knowing that the primary juristic purpose of the mobile network data is to test the criminal hypothesis on the basis on its pertinence, rather than on the number of different data types included in a case. However, the mobile data relevance naturally builds upon the mobile network data variety, recalling the discussion on its actual role in processing the criminal offenses presented in Table 43. For the minimum variety cases - that is Case I, II, III and VII - the prosecution requested the movement behavior profiling, the service usage behavior profiling, and critical calling events are sufficient to test the hypothesis alone. For the remaining cases, they combined the mobile data types to reinforce their argument, reckoning that the complementary nature of the data types enables better reconstruction of the criminal events for each of the target identities investigated. In Case IV this action enabled more substantive reconstruction of the drug production and trade scheme, and in Case V and VI of the human trafficking scheme. Consequently, the mobile data relevance was the feature pointed in the final case disposition reports, which implicitly abstracts the mobile data variety contribution in the case processing.

This line of reasoning is further corroborated when the relationship of the mobile data variety and the case disposition time are analyzed without the outlier Case III. The difference in the overall processing for the cases where the localization and network-management data are included separately, and when they are combined with the content-of-communication data suggest that while the variety reinforces the legal argument, in the same time prolongs courtroom processing. Particularly, the criminal hypothesis testing takes less time when only the movement or service activity profiles are contrasted with the remaining evidence than in the instance when the critical conversational parts are additionally introduced to reinforce the reconstruction of the criminal events. The reinforced reconstruction extends the courtroom processing time – and with that the case disposition - in that requires additional time for presenting and discussing the content-of-communication details in the context of the criminal events.

## 5.2. Mobile Network Data Volume Contribution – Discussion

### 5.2.1. Localization Data

The first row in Table 36 does not indicate a statistically significant correlation either between the localization data and the separate case disposition segments or with the case disposition time overall. In the context of the localization data volume contribution in the case processing performance, the negative correlation between the number of localization records and the case disposition time might be an indication of a faster case processing with a larger number of localization records.

With the main juristic purpose of the localization data is to provide evidence as to the movement behavior for the target identity of interest, this outcome is expected considering the juristic actors' interest in the relevance of the mobile network data (section 5.1.3). That is, the more localization records are used in developing the movement behavior, the better is the granularity in reconstructing the criminal events. The better granularity, in turn, maximizes the conclusiveness of the localization evidence, which in turn eliminates (or minimizes) the potential challenges to the legal argument. Having a strong and conclusive outcome of the criminal hypothesis testing provides the ruling judges a sufficient argument to dispose the case faster, which indeed is observed as a trend for the localization data in this study. This observation cannot be formally generalized given the statistical insignificance of the results and the small number of cases, however, the conclusions align with the relevance-based contribution of the localization data in the case processing performance, noted in section 4.4.3.

### 5.2.2. Network-management Data

The first row in Table 36 does not indicate a statistically significant correlation between the network-management data and the forensic processing segments, but there is a statistically significant strong negative correlation for the juristic processing segment and the case disposition overall. As noted in section 4.3.5.5 and 4.4.1, the negative correlation is characteristic for all mobile network data types, having the number of target identities, the investigation timespan and the actors involved influencing the impact of the network-management data volume on the time needed to be brought in forensic custody. In the examination and analysis segment, the confounding set of factors was identified in the number of target identities and the moderate compliance with the 3GPP and ISO/IEC SC 27 recommendations for data formatting and evidence handling (section 4.4.2). The strong negative correlation between the network-management data and the examination and analysis time – although not statistically significant – hints their importance for the concluding segments of the overall case disposition process.

In this direction, the statistically significant strong and negative correlation between the network-management data and the juristic processing time and the case disposition time (second part of the second row in Table 36) suggest that the case processing in fact is faster when a large number of localization records are used as evidence. Given that the network-management data are also a non-real time type of data (as the localization records), the rationale from the previous section holds here too.

With the main juristic purpose of the network-management data is to provide evidence as to the service activity behavior for the target identity of interest, it is expected that judges would capitalize on the finely granular service behavior profiling to dispose the cases in a less number of days. That is, the more network-management data records are used in developing the service activity behavior, the better is the granularity in reconstructing the criminal events. The better granularity, in turn, maximizes the conclusiveness of the network-management evidence, which in turn eliminates (or minimizes) the potential challenges to the criminal hypothesis. The statistical significance of the results in this case in fact reinforces the conclusions previously drawn for the localization data, and also for the non-real time data in general. The reason that prevented a statistically significant negative correlation for the localization data– next to the smaller sample size – is related to the innate probative value of these data types.

### 5.2.3. Content-of-communication Data

The third row in Table 36 does not indicate a statistically significant correlation between the content-of-communication data and the forensic processing segments, but there is a statistically significant strong positive correlation for the juristic processing segment and the case disposition overall. As noted in section 4.3.5.5 and 4.4.1, the negative correlation is characteristic for all mobile network data types, having the number of target identities, the investigation timespan and the actors involved influencing the impact of the network-management data volume on the time needed to be brought in forensic custody. In the examination and analysis segment, the confounding set of factors was identified in the number of target identities and the moderate compliance with the 3GPP and ISO/IEC SC 27 recommendations for data formatting and evidence handling (section 4.4.2). The positive correlation between the content-of-communication data and the examination and analysis time – although not statistically significant – hints at their importance for the concluding segments of the overall case disposition process.

The statistically significant correlation between the content-of-communication data and the juristic processing time and the case disposition time (second part of the third row in Table 36) suggest that the juristic actors are in fact using the critical conversational parts extracted out of the intercepted data to expedite the courtroom processing of the cases. The positive correlation is logical, given that these parts must be replayed in courtroom in presenting the evidence (in contrast, the network-management or the localization data are aggregated in a service activity or movement behavior profile and presented as such). Moreover, the granularity for the content-of-communication data is improved by increasing the number of critical conversational segments selected and presented as evidence. Following this line of reasoning as for the previous two data types, the more granular representation of suspects communication  maximizes the conclusiveness of the content-of-communication evidence, which in turn eliminates (or minimizes) the potential challenges to the criminal hypothesis.

## 5.3. Forensic Processing Contribution – Discussion

Interested to explore the general relationship between the forensic processing and the overall case disposition, Table 41 summarizes the Pearson’s correlation coefficients for each of the case processing segments and the overall case disposition time. The statistically significant positive correlation is an expected outcome for the examination and analysis and the juristic processing segments, because the previous one is where the probative value of the mobile network data is extracted, and the latter is where this value is applied in the criminal hypothesis testing, which essentially is the concluding action that definitely disposing the cases.

The statistically significant positive correlation for the examination and analysis segment suggest that the cases are disposed in correlation to the time needed for the mobile data to be forensically processed. Recalling the statistically significant ANOVA for the mobile data variety and the examination and analysis time (without the outlier), it was found that each data type needs different time to be processed, and even more, each combination of more than one data types also needs different time for the data to be consolidated based on the target identities identified. In addition, it was found that the cases including content-of-communication data tend to consume more examination and analysis time. That this holds true, Figure 10(b) indeed shows a higher examination and analysis times for this subset of cases (that is, Case IV, V, and VI).

Coupling this information with the correlations in sections 4.3.5, it follows that the negative correlational trend between the volume and the time need for forensic processing of the non-real time mobile network data is preponderated when they are combined with the content-of-communication data, given the positive correlation between the content-of-communication data and the examination and analysis time. . Having also a positive correlation between the content-of-communication data and the case disposition time (section 4.3.4.5.3), the positive correlation is logical for these cases, given that cases with a larger case disposition time include fewer network-management and/or localization data records.

For the network-management minimum variety cases (Case II and Case VII), both the examination and analysis time and the case disposition time are in correlation to the number of network-management records included, supporting the general statistically significant positive correlation achieved. For the content-of-communication minimum variety case (Case III) both the examination and analysis time and the case disposition time are in correlation with the hours of content-of-communication, again supporting the general statistically significant positive correlation achieved. Lastly, for the localization data minimum variety case (Case I) which has the minimum number of localization records, both the examination and analysis time and the case disposition time are the second minimum ones, following the general trend of a positive correlation.

The statistically significant positive correlation for the juristic processing segment is expected for the overall sample (p =0.001) on the accounts that the juristic processing effort is what concludes the case to an end (i.e., the correlation achieved confirms the conclusions reached as for the mobile network data forensic processing).

## 5.4. Implications for Action

The significance of the research problem is associated with the threat of case processing performance degradation in Macedonia due to the emerging trend of mobile-enabled crimes. In reference to section 2.2, Macedonian criminal justice system ranks 11st out of 17 criminal justice systems assessed by the European Commission for the Efficiency of Justice with a case disposition time of 211 days on average. According to the Figure 1 in section 2.1.4, the current capacity for criminal justice delivery summarizes to a 99.735% smaller budget and a 97% larger case log compared to the European average (number of criminal cases/per 100.000 inhabitants) where each judge needs to process four times more criminal cases than their European colleagues for a six-time smaller remuneration. Consequently, the current case processing practice needs to *adopt* in way that will prevent the exponential growth rate of mobile-related crimes to extend the case disposition time and with that to cause an institutional collapse (Cisco, 2015; UNODC, 2013).

To facilitate this adaptation, this section discusses the results from this study using the IAD framework to identify the implications for the practice as of the physical and material conditions, community attributes, and rules-in-use. Next to the institutional part, the results are also discussed to emphasize the implications for future research in the domain of mobile-related criminal case processing.

### 5.4.1. Implications for Practice

#### 5.4.1.1. Physical and Material Conditions

In reference to the first column of the exploratory matrix in Figure 7, the implications in regards the present physical and material conditions are mainly directed towards the budgetary appropriations for both the forensic processing and juristic processing support. According to the evaluation from section 2.1.1.4, the NDFL is still not accredited with the ISO/IEC 17025 standard for competence and conformity of forensic laboratories (International Standardization Organization, 2005), and neither the literature nor the case data indicated that the laboratory possesses any specialized software solution for examination, analysis and interpretation of mobile network data. In conjunction with the positive correlation between each segment of the mobile-enabled criminal case processing and the case disposition time, the benefits of the ISO 17025 accreditations and use of a specialized software for forensic management of mobile network data can be seen in an improved data sorting, aggregation, interlinking, map rendering, and multiple source data consolidation within the examination and analysis segment. With such an ability, the NDFL can improve its effectiveness in mobile network production and decrease the examination and analysis time for a given volume or variety set of mobile network data. The decreased examination and analysis time will result in a decreased case disposition time as indicated in section 4.3.6.2, which aligns well with the imperative to minimize the time needed for a criminal case to be brought to an end.

As of the juristic processing support, Figure 1 indicate that the Macedonian administrators of justices need to process four times more criminal cases than their European colleagues for which they receive a six-time smaller remuneration. In addition, the evaluation from section 2.1.1.2 reveals that the remuneration is -12.1% of the national average gross salary. The appreciation of their societal role through an adequate remuneration is a necessary prerequisite in the effort to optimize the case disposition time, given that the judges are the ultimate decision-makers that determine the time and the verdict that brings a criminal case to an end (this point is further discussed in the subsequent section). In the context of the mobile-enabled crime, this implication can be seen towards a decreased juristic processing time, where the financial compensation can contribute for a more structural approach in the application of the mobile network evidence, which is found not to be a case for this study considering the average of 151.857 and standard deviation of 101.45 juristic processing days from Table 11.

#### 5.4.1.2. Community Attributes

In reference to the second column of the exploratory matrix in Figure 7, the implications in regards the present community attributes are directed towards the acquisition and delivery procedure, the forensic methodologies, and judges' familiarity with the basic structure and probative value of the mobile network data. As of the acquisition and delivery procedure, the main recommendation for further enhancement is the implementation of the 3GPP lawful interception infrastructure (3rd Generation Partnership Project, 2015a). Being able to authorize and authenticate the evidence source over the HI1 interface, the prosecution can coordinate the acquisition and delivery procedure by defining the correlational number for the target identities it needs multiple data types. Using this number in the records and the standardized format prescribed for the HI2 and HI2 interfaces, the operators and the NLEA can provide 3GPP-compliant localization, network-management, and content-of-communication data.

The 3GPP lawful interception is important considering the positive correlation between the acquisition and delivery time and the case disposition time because it will enable the prosecution to eliminate the unnecessary time when collecting multiple mobile network data types. It can also provide with an opportunity to transfer NLEA functionality to the operators for medium and/or maximum variety cases for the target identities associated with their networks, which in turn will enable aggregated data collection per each target identity and investigation timespan. Having a distributed evidence acquisition and delivery architecture can help the prosecution to better organize the time needed to collect mobile network data – either per offense type, mobile data type, set of target identities, or investigation periods - and with that to help minimize the case disposition time.

The full 3GPP compliance is equally important for both the acquisition and delivery and the examination and analysis processes. Together with the implementation of the prescribed 3GPP handover interfaces, it is prerequisite for an effective multi-jurisdictional collaboration and adequate response to the so-called “European investigation order” (Gruodyt & Bilius, 2014; Ruggeri, 2013). Together with the ISO/IEC SC27 compliance, the examination and analysis can benefit from the comprehensive 3GPP formatting in that can minimize the time needed for the evidence to be forensically consolidated, eliminate any uncertainties associated with its probative value, assures fully-compliant cross-jurisdictional evidence delivery as noted above.

Being able to improve the data consolidation, the NDFL practitioners can minimize the time needed to interpret the data and produce the requested mobile network evidence more quickly. The improved reliability of the mobile network data increases the confidence in its probative value, providing an opportunity for the judges to dispose the case in a shorter period of time while preserving the quality of the judicial allocation. The fully-compliant cross-jurisdictional evidence delivery will enable the NDFL to collaborate with digital forensic laboratories in other jurisdictions and also receive an evidence in a fully compliant 3GPP format from other jurisdictions such as in Case VII.

In reference to section 2.3, the purpose of the ISO/IEC SC27 compliance is twofold – first, it assures that that the deliverable out of the digital forensic investigation is of utmost relevance for the criminal case processing, and second, enable use of a common investigation instrument across various operational scenarios involving mobile network data. The relevance of the movement/service activity behavior profiles and conversational excerpts has already been noted to increase the confidence for the juristic actors to utilize the mobile network data in the case processing performance.

The benefits of a common investigation instrument – or the harmonized digital investigation schema prescribed in the ISO/IEC 27043 *Incident Investigation Principles and Processes* document - refer to the "human error minimization, balance between the investigative time constraints, costs, and evidentiary weight, and cross-border cooperation" (International Standardization Organization, 2014d). In the context of the case processing performance improvement, the use of this model clearly will eliminate the observed fluctuations in the examination and analysis time (section 5.1.2).

In reference to section 2.1.2, the Academy of Judges and Prosecutors is responsible for providing the cybercrime training needed for the operational processing of the emerging crime. Considering the current lack of dedicated modules covering the basic structure and probative value of the mobile network data together with the average of 197.571 and standard deviation of 118.337 case disposition days from Table 11, it follows that mobile related cases are disposed mainly on judges 'subjective degree of comfort and familiarity with the associated evidence. Therefore, an extension in the Academy of Judges and Prosecutors curricula towards the nature of the mobile-enabled crime is the main recommendation as to structure the application of the mobile network evidence and with that to optimize the case disposition time.

The extension can benefit from the results in this study by pointing out how each of the mobile network data types affect different segments of the case processing in the recent practice as elaborated in the first part of this chapter. Knowing the uncertainty associated with the localization records, the judges in collaboration with the prosecution may request additional content-of-communication data to reinforce the legal argument. On the similar account, the network-management data can be prioritized in the case processing practice as the mobile data type with a high degree of conclusiveness, no uncertainty associated, and negatively correlated with the case disposition time when acquired in larger volumes.

### 5.4.1.3. Rules-in-use

In reference to the third column of the exploratory matrix in Figure 7, the implications in regards the present rules-in-use are directed towards the regulative changes prescribing implementation of the 3GPP compliant evidence collection architecture and the legislative changes prescribing time limits for evidence delivery response, required ISO/IEC SC27 compliance, extension of the NLEA functionality, and formal application of the mobile network data as juristic evidence.

The current regulative prescriptions from the Electronic Communication Law and the Telecommunication Interception Law have not indicated a mandatory implementation of the 3GPP lawful evidence collection architecture, nor did the case data suggest that actors involved have optionally implemented it. In order the recommendations for this architecture noted in the previous two subsections to take effect, the regulative framework must direct the involved actors about its implementation and intended use. Therefore, the recommendation for the rules-in-use is to adjust the current regulation as to oblige the local operators and the NLEA to implement the 3GPP lawful evidence collection architecture. This provision will also make the full 3GPP evidence formatting a compulsory requirement, which will enable the prosecution to decrease the acquisition and delivery time – by imposing time limits for the involved actors to deliver the requested evidence - and more important, the NDFL to decrease the examination and analysis time by optimized evidence consolidation and probative value extraction. Recalling the positive correlations in section 4.3.6, this will effectively decrease the case disposition time for the mobile-enabled crime cases.

In support to the optimized forensic processing are the legislative adjustment as of compulsory use of the ISO/ISC 27 methodologies and the ISO 17025 accreditation of the NDFL. Towards the imperative for decreased case disposition time, the compulsory ISO compliance will structure the evidence analysis by minimization of the human error and balancing between the investigative time constraints, costs, and evidentiary weight, which in turn, will decrease the time needed the mobile network data to be forensically processed. In addition to associated decrease in the case disposition time, the ISO compliance will enable legally-supported and effective cross-jurisdictional collaboration.

Another benefit of the compulsory 3GPP and ISO compliance is the possibility to extend the NLEA functionality to be performed by the local operators. Enabling a distributed and 3GPP-compliant evidence collection architecture in coordination with a fully ISO-compliant NDFL will prevent the mobile network data volume and variety to be moderated by the confounding factors elaborated in section 4.4 and with that will help the juristic actors to better organize the case processing from start to an end. For the better organization of the case processing, the Criminal Procedure Code and the Criminal Code can possibly be adjusted to include provisions for a formal application of the mobile network data as juristic evidence. In reference to the results of this study, this encompasses the use of the network-management and the content-of-communication data for a formal case conclusion on the basis on their probative value, maximum conclusiveness, and relevance to the legal argument for certain offense types.

## 5.4.2. Implications for Future Research

### 5.4.2.1. Physical and Material Conditions

In reference to the present physical and material conditions from Figure 7, the implications for future research are to explore the effect of the case load/remuneration on judges' decision to dispose certain mobile-enabled case. That is, judges' might be surveyed to provide their opinion on how their motivation and workload shape the use of the mobile-network data to resolve given criminal offense. A similar survey might be executed among all the actors involved in the acquisition and delivery and examination and analysis to determine whether and how their current workload, financial compensation, and working tools affect the time they need to delivery or process the mobile network data.

### 5.4.2.2. Community Attributes

As of the community attributes from Figure 7, the aforementioned surveys on the financial and workload stimulus might also be used to render what are the main incentives/deterrents for each of the actors involved to contribute in the optimization of the case processing process and decrease in the case disposition time. This encompasses training, collaboration, increased interaction between the operators, forensics actors and the administrators of justice, protection, safety, work-related stress, or other societal aspect of their involvement in the mobile-enabled case processing.

In the context of the confounding factors in this study, the future research courses encompass exploration of effect of the number of target identities, investigation timespan, full 3GPP compliance, and full ISO compliance on the acquisition and delivery time, examination and analysis time, juristic processing time, and the overall case disposition time. Assuming a larger case sample for all of the aforementioned research scenarios, the study can also be repeated to gather a more precise information on the relationship between the mobile network data volume, variety and forensic processing and each of the segments of the criminal case processing.

The factors affecting the forensic processing segments – mainly the number of target identities and the investigation timespan – can also be taken to complement the set of independent variables as to understand how each of the aspects of the mobile network data that moderate each of the case processing segments. Next to them, the full 3GPP and ISO compliance can be added as intervening factors to assess and compare the performance in the acquisition and delivery, examination and analysis, juristic, and case processing time with the results gather in this study.

In the context of the results of this study, a further inquiry of the statistically significant ANOVA in section 4.3.4.2 is needed to understand the impact of the number of data types included in a case on the analysis and examination time, as well as on the case disposition time. The same holds for the t-tests, where the interesting difference observed in the overall processing for the cases where the localization and network-management data are included separately, and when they are combined with the content-of-communication data needs to be explored to reveal the exact relationship. Similarly, the correlational coefficients in Table 36 can be recalculated for a larger sample to explore the effect of the volume of each data type on the acquisition and delivery time and the examination and analysis time. The same calculations can be taken to further explore the relationship between the localization data and each segment of the criminal case processing.

#### 5.4.2.3. Rules-in-use

As of the rules-in-use from Figure 7, the aforementioned surveys might additionally be extended to understand which rules-in-use affect them and how the can be change towards the optimization of the case processing process and decrease in the case disposition time. In the context of the confounding factors and the results in this study, the future research courses encompass exploration of effect of the 3GPP compliant evidence collection architecture, prescribed time limits for evidence delivery, extension of the NLEA functionality, and the formal juristic application of the mobile network data.

The effect of a fully-complainant 3GPP evidence collection architecture can be assessed for the same set of research variable and then compared with the results from this study to understand whether an improvement in the processing time is possible and which segment it can be achieved. Similarly, the time limits on the evidence delivery can be explored in terms of more structured acquisition and delivery time, and whether that can be translated in a decreased case disposition time as suggested with the positive correlation from section 4.3. The extension of the NLEA functionality can be supported by a future research that compares the findings as of the relationship when the NLEA is central authority for content-of-communication data collection, and when this is performed by each operator for the target identities being registered on its network.

For the formal juristic application of the mobile network data, the study can be extended to explore the contribution of the mobile network data for certain offense types, or for a given class of criminal cases of particular interest for the Macedonian criminal justice system authorities. Alternatively, the impact of the mobile data types when combined with the remaining evidence of various types and classes of offences, not just the ones in the convenience sample, can also be explored.

## 5.5. Concluding Remarks

The research inquiry undertaken in this study is an inaugural effort to explore the contribution of the localization, network-management, and content-of-communication data as a juristic evidence. Motivated to identify how each of these data types are used in the case processing, the Macedonian criminal justice system was selected as one with the highest risk of institutional collapse in face of the rapid growth in mobile-enabled crimes.

Their contribution was approached from two perspectives, one is the number of data types included in a criminal case as evidence, and the other is the volume of each of these data types. The rationale behind this choice of independent variables is that these are the basic aspects framing the probative value and the relevance of the mobile network data in general. Knowing that the mobile data needs to be collected and its probative value extracted and interpreted in order to be admitted and applied as juristic evidence in the criminal case processing, the acquisition and delivery time and the analysis and examination time were selected as intervening variables rendering the associated effort. Following the implications for institutional collapse of the Macedonian criminal justice system suggested by the European Commission for the Efficiency of Justice, the dependent variable was chosen to be the same as the one used in their juridical evaluation - the case disposition time -or the time needed for a case to be brought to an end.

For a mobile-enabled crime case to be brought to an end, the decision-makers need to utilize the mobile network data as juristic evidence in testing the associated criminal hypothesis and rendering the final verdict. The results from this study indicate that the case disposition is in fact expedited by the network-management and the content-of-communication data. In the previous instance, the relevance of the network-management data was recognized in the highly granular service behavior profile developed using larger number of records, while in the later instance the relevance of the content-of-communication data was recognized in the substantial number of excerpts of intercepted communication. The results also indicate that the number of mobile network data types impacts the case disposition, however the small sample size prevented this study to fully capture the mobile network data variety effect.

The study in effect shows that the mobile network data has a practical and relevant contribution in criminal case processing in Macedonia. Given the burgeoning trend in cross-jurisdictional mobile-enabled crimes, the mobile-network data will play a dominant role in the forthcoming case processing practice, emphasizing the importance of the findings for a timely reorganization and adjustment of the practice in preparing a better judicial response towards the emerging crime. On this account, the implications for future research enlist several interesting aspects for a more in-depth exploration of entire juristic context in which the mobile network data bears a relevance in the case processing. In any respect, the output of this particular study is practically useful in preliminary understanding of the mobile-enabled criminal case processing.

# REFERENCES

# REFERENCES

3rd Generation Partnership Project. (2002). 3GPP TS 23.002 V3.6.0 -- Technical Specification Group Services and Systems Aspects -- Network architecture (Release 99). 3GPP. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2007). 3GPP TS 21.11 V8.14.1 -- Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 1999). 3GPP. Retrieved from http://www.qtc.jp/

3rd Generation Partnership Project. (2008). 3GPP TS 23.002 V7.6.0 -- Technical Specification Group Services and Systems Aspects -- Network architecture (Release 7). 3rd Generation Partnership Project. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2012). 3GPP TS 21.111 V11.0.1 -- USIM and IC Card Requirements (Release 12). 3GPP. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2013). *Vocabulary for 3GPP Specifications*. 3GPP. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2014a). 3GPP TS 23.003 -- Numbering, addressing and identification (Release 12). Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2014b). 3GPP TS 32.298 -- Telecommunication management -- Charging management -- Charging Data Record (CDR) parameter description (Release 12). 3rd Generation Partnership Project. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2014c). 3GPP TS 32.299 -- Telecommunication management -- Charging management -- Diameter charging applications (Release 12). 3rd Generation Partnership Project. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2014d). 3GPP TS 33.106 -- 3G security --Lawful Interception requirements (Release 12). 3GPP. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2014e). 3GPP TS33.107 - 3G security -- Lawful interception architecture and functions (Release 12). 3GPP. Retrieved from http://www.3gpp.org/

3rd Generation Partnership Project. (2015a). 3GPP TS 33.107 V13.0.0 --3G security -- Lawful interception architecture and functions (Release 13). Sophia Antipolis Cedex: 3GPP.

3rd Generation Partnership Project. (2015b). 3rd Generation Partnership Project -- Evolved Universal Terrestrial Radio Access (E-UTRA) -- LTE Positioning Protocol (LPP) (Release 12). Sophia Antipolis Cedex: 3GPP.

Aligica, P. D., & Tarko, V. (2013). Co-Production, Polycentricity, and Value Heterogeneity: The Ostroms' Public Choice Institutionalism Revisited. *American Political Science Review*, *107*(04), 726–741. doi:10.1017/S0003055413000427

Assembly of the Republic of Macedonia. (1991). *The Constitution of the Republic of Macedonia*. Retrieved from http://www.sobranie.mk/ustav-na-rm.nspx

Assembly of the Republic of Macedonia. (2008a). *Criminal Procedure Law*. Retrieved from http://www.pravda.gov.mk/documents/zkp_posledna_verzija_26.pdf

Assembly of the Republic of Macedonia. (2008b). Public Prosecution Act. Skopje, Republic of Macedonia: Assembly of the Republic of Macedonia.

Assembly of the Republic of Macedonia. (2010). The Code of Practice for Forensics Science. Skopje, Macedonia: GPO. Retrieved from http://www.bsv.gov.mk/

Assembly of the Republic of Macedonia. (2013). Criminal Code of The Republic of Macedonia. Skopje, Macedonia: GOP. Retrieved from http://www.legislationline.org/documents/action/popup/id/16066/preview

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics*. Gaithersburg, MD. doi:10.6028/NIST.SP.800-101r1

Bell, J. (2006). *Judiciaries Withing Europe*. Cambridge, UK: Cambridge University Press.

Besanko, D., & Braeutigam, R. (2010). Externalities and Public Good. In *Microeconomics* (pp. 1–822). Hoboken, New Jersey: John Wiley & Sons.

Besley, T., & Ghatak, M. (2006). Public Goods and Economic Development. In A. V. Banerjee (Ed.), *Public goods and economic development* (pp. 285 –318). New York, NY: Oxford University Press.

Blank, A. (2011). The Limitations and Admissability of Using Histroical Cellular Side Data to Track the Location of a Cellular Phone. *Richmond Journal of Law & Technology*, *XVIII*(December), 1–43.

Brenner, S. W. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston, MA: Northeastern University Press.

Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law and Social Change*, *54*(5), 339–357. Retrieved from http://link.springer.com/10.1007/s10611-010-9261-6

Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences*, *54*(6), 1353–1364. doi:10.1111/j.1556-4029.2009.01150.x

CEPEJ. (2014). *Evaluation of European Judicial Systems* (Vol. 2014). Brussels, Belgium. Retrieved from http://www.coe.int/t/dghl/cooperation/cepej/evaluation/2014/Rapport_2014_en.pdf

Cisco. (2015). *Cisco Visual Networking Index : Global Mobile Data Traffic Forecast Update , 2014 – 2019*. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

Clark, E., & Gibbs, D. (2001). Wireless Network Analysis. In E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology* (pp. 1–448). Academic Press.

Cole, G. F., & Smith, C. E. (2006). *The American System of Criminal Justice* (11th ed.). Belmont, CA: Wadsworth Publishing.

Cox, C. (2014). *An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications* (Second.). New York, NY: Wiley.

Dubois, E., Schurrer, C., & Velicogna, M. (2013). *The functioning of judicial systems and the situation of the economy in the European Union Member States*. Strasbourg, France. Retrieved from http://ec.europa.eu/justice/effective-justice/files/cepej_study_justice_scoreboard_en.pdf

Ericcson. (2015). *Ericsson Mobility Report*. Stockholm, Sweden. Retrieved from http://hugin.info/1061/R/1925907/691079.pdf

European Network of Forensic Science Institutes. (2009). Guidelines for Best Practice in the Forensic Examination of Digital Technology. Retrieved from http://www.enisa.europa.eu/activities/cert/support/exercise/files/

Forte, D., & Donno, A. de. (2010). Mobile network Investigations. In E. Casey (Ed.), *Handbook of Digital Forensics and Investigation* (pp. 517–567). Burlington, MA: Elsevier.

Glisson, W. B., Storer, T., & Buchanan-Wollaston, J. (2013). An empirical comparison of data recovered from mobile forensic toolkits. *Digital Investigation*, *10*(1), 44–55. doi:10.1016/j.diin.2013.03.004

Gruodyt, E., & Bilius, M. (2014). Investigating Cybercrimes: Theoretical and Practical Issues. In *Regulating eTechnologies in the European Union* (pp. 217–249). New York: Springer.

Hammergren, L. (2011). Judicial Governance and the Use of ICT. *Buenas Prácticas Para La Implementación de Soluciones Tecnológicas En La Administración de Justicia*, 7. Retrieved from http://www.iijusticia.org/docs/Linn.pdf

Helfenstein, S., & Saariluoma, P. (2014). How Cyber Breeds Crime and Criminals. In *DigitalSec 2014 Proceedings:The International Conference on Digital Security and Forensics* (pp. 76–90).

Herbert, D. J. (2014). Scientific Fact of Junk Science? Tracking a Cell Phone without GPS. *Judges' Journal*, *53*(1), 37–39. Retrieved from http://www.americanbar.org/publications/judges_journal/2014/winter.html

International Standardization Organization. (2005). ISO/IEC 17025:2005 -- General requirements for the competence of testing and calibration laboratories. Geneva, Switzerland. Retrieved from http://www.iso.org/

International Standardization Organization. (2012). ISO/IEC 27037:2012 guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from http://www.iso.org/

International Standardization Organization. (2014a). ISO/IEC 27042 -- Guidelines for the analysis and interpretation of digital evidence. Geneva, Switzerland. Retrieved from http://www.iso.org/

International Standardization Organization. (2014b). ISO/IEC 27043 -- Incident investigation principles and processes. Geneva, Switzerland. Retrieved from http://www.iso.org/

ITU Cybersecurity Division. (2009). Understanding Cybercrime: A Guide for Developing Countries. Geneva, Switzerland: ITU.

Marshall, A. M. (2011). Standards, regulation & quality in digital investigations: The state we are in. *Digital Investigation*, *8*(2), 141–144. doi:10.1016/j.diin.2011.11.001

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation*. San Francisco, CA: Jossey-Bass.

Ministry of Justice of the Republic of Macedonia. (2005). Criminal Procedure Code of the Republic of Macedonia. Skopje, Republic of Macedonia: Ministry of Justice. Retrieved from http://makemigration.readyhosting.com/upload/krivicnapostapka.pdf

Ministry of Justice of the Republic of Macedonia. (2007). ICT Strategy in Macedonian Justice. Skopje, Republic of Macedonia: Ministry of Justice. Retrieved from http://www.coe.int/t/dghl/cooperation/cepej/profiles/FyromJICTStrategy_en.pdf

O'Malley, T. A. (2011). Using Historical Cell Site Analysis Evidence in Criminal Trials. *United States Attorneys Bulletin*, *59*(6), 16–34.

Ostrom, E. (2005). *Understanding Institutional Diversity*. Princeton, NJ: Princeton University Press.

Ostrom, E. (2007). Institutional rational choice: An assessment of the Institutional Analysis and Development Framework. In P. Sabatier (Ed.), *Theories of the Policy Process* (2nd Editio., pp. 21–64). New York, New York, USA: Westview.

Palmer, G. (2001). *A Road Map for Digital Forensic Research*.

Perry, A. J., & Carter, A. (2011). Computer Crimes. *American Criminal Law Review*, *41*(2), 313 – 367.

Phelan, C., & Wren, J. (2002). *Exploring reliability in academic assessment*. *UNI Office of Academic Assessment*. Retrieved June 22, 2015, from https://www.uni.edu/chfasoa/reliabilityandvalidity.htm

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S1742287614001066

Rajamaki, J., & Knuuttila, J. (2013). Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement. In *2013 European Intelligence and Security Informatics Conference* (pp. 198–203). IEEE.

Riege, A. (2003). Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative Market Research: An International Journal*, *6*(2), 75–86. doi:10.1108/13522750310470055

Ruggeri, S. (2013). Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality. In *Transnational Evidence and Multicultural Inquiries in Europe* (pp. 52–65). doi:10.1007/978-3-319-02570-4

Salzberger, E. (1993). A Positive Analysis of the Doctrine of Separation of Powers, or : Why Do We Have an Independent Judiciary ? *International Journal of Law and Economics*, *13*(1), 349–379.

The Council of the European Union. (2001). Convention on Cybercrime. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

The Council of the European Union. (2006). DIRECTIVE 2006/24/EC. *Official Journal of the European Union*, *1*(March 2004), 54–63. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

The European Commission for the Efficiency of Justice. (2013). *Evaluation of European Judicial Systems*. *Evaluation of European Judicial Systems*. Retrieved from http://www.coe.int/t/dghl/cooperation/cepej/evaluation/default_en.asp

UNODC. (2013). *Comprehensive Study on Cybercrime*. Retrieved from http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

UNODC, & UNECE. (2012). *Principles and Framework for an International Classification of Crimes for Statistical Purposes*. Geneva, Switzerland.

Wells, A. (2014). Ping! the admissibility of cellular records to track criminal defendants. *Saint Louis Public Law Review*, *33*(1), 487–518.

Willassen, S. Y. (2003). Forensics and the GSM mobile telephone system. *International Journal of Digital Evidence*, *2*(1), 1–17.

Zvrlevski, M., Andonova, S., & Miloshevski, V. (2014). *Handbook of Computer Crime for Legal Practitioners*. Skopje, Republic of Macedonia: OSCE.

# VITA

# VITA

- Name: Filipo Sharevski
- Web page: https://www.cerias.purdue.edu/site/people/students/view/1289

Work Experience:

- May 2013 – present: Teaching Assistant (Contemporary Problems in National Cybersecurity class); Research Assistant (INSURE and REU Projects), Purdue Polytechnic Institute, Purdue University, USA

- July 2009 – August 2012: Core Service Network - Intelligent and Prepaid Network Support Systems Engineer, Vip Operator Macedonia, mobile network operator, member of Telekom Austria Group, Vodafone partner

- January 2008 – January 2009: Institute of Telecommunications, FEEIT Skopje – Teaching and Research Assistant (Information Theory and Security in Telecommunications classes)

Education:

- August 2012 – December 2015: PhD Studies, Interdisciplinary Ph.D. Program in Information Security , CERIAS (http://www.cerias.purdue.edu/), Purdue University, GPA 3.93 - Summa Cum Laude, Dissertation: “The Impact of Mobile Network Forensics Evidence on the Criminal Case Processing Performance in Macedonia: An Institutional Analysis”, Advisor: Prof. Mellissa J. Dark

- October 2008 – July 2009: Master Studies in Communication and Information Technologies, “Faculty of Electrical Engineering and Information Technologies” – Skopje (http://tk.feit.ukim.edu.mk/), GPA 4.00 - Summa Cum Laude, Thesis: “Security and Privacy Enhancement Mechanisms on PHY and MAC Layer in RFID Based Systems ”, Mentor: Prof. Dr. Aleksandar Risteski

- October 2004 - July 2008: Graduate Studies, “Faculty of Electrical Engineering and Information Technologies” – Skopje, date: 01.07.2008, mean degree: 9.15, Diploma Thesis: “Quality of Service in Mobile Networks” Mentor: Prof. Toni Janevski

Research career:

- INSURE Project (research assistant)– A collaborative research among four successful and mature Centers of Academic Excellence in Information Assurance Research (CAE-R) and the National Security Agency (NSA), the Department of Homeland Security and other federal agencies that includes both unclassified and classified research problems in cybersecurity. This work is funded by NSF Award No. 1344369. Web page: http://insurehub.org/about-us

- REU Project (research assistant): The CERIAS Information Security REU Program provides the opportunity for undergraduate students to engage in the forefront of information security research working on individual project areas and supported by the NSA, DHS and other federal agencies. This work is funded by NSF Award No. 1062970. Web Page: https://www.cerias.purdue.edu/site/reu/

- RiWCOS Project (research collaborator) – Interoperability in heterogeneous wireless networks through a flexible wireless reconfiguration policies. This work was funded by the NATO SfP-982469 Award.

Grants, fellowships and Awards:

- January 2014: Second Place on the Cyber 9/11 Challenge Competition – Atlantic Council, Washington D.C. USA

- September 2012: First national fellowship for Ph.D. students on the top 100 world universities on the Shanghai University ARWU ranking (2012)

- June 2011: Best employee in Vip Operator for May 2011

- May 2009: IEEE International Telecommunication Forum – TELFOR 2008, Best Young Researcher for paper „Performance Analysis of Routing Protocols In Ad Hoc and Sensor Networking Environments“

Engineering experience:

- Mobile Network Related Products: Cyber-enabled Fraud Management System – Telecom Austria Group; Network Quality Monitoring – Vip Operator

- Programming Languages: C/C++, Perl, Python, PhP Java, CySeMoL

Scientific interests:

- Complex networks cybersecurity (mobile networks, critical infrastructure), cyber resilience, intrusion tolerance, moving target defense mechanisms, digital forensics, and cyber warfare.

# PUBLICATIONS

# PUBLICATIONS

Sharevski, F. (2013). Digital forensic investigation in cloud computing environment: Impact on privacy. In M. Losavio (Ed.), *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)* (pp. 1–6). Hong Kong: IEEE. doi:10.1109/SADFE.2013.6911542

Manfredi, V., Sharevski, F., & Dark, M. J. (2013). Random Packet Size Morphing and Direct Target Sampling for VoIP Language Obfuscation. In *Grace Hopper Celebration of Women in Computing*. Minneapolis, MN: ACM.

Dietz, E., Kirby, A., Sharevski, F., & Ankhlam, C. (2014). Applied Engineering Models Suggesting Strategies to Reduce Causalities During a School Active Shooter Event. In *4th IAJC/ISAM Conference Proceedings* (pp. 1–12). Orlando, Florida: IAJC. Retrieved from http://cd14.ijme.us/papers/143__Eric Dietz, Adam Kirby, Charles Anklam, Filipo Sharevski.pdf

Ankhlam, C., Kirby, A., Sharevski, F., & Dietz, J. E. (2015). Mitigating Active Shooter Impact; Analysis for Policy Options Based on Agent/Computer Based Modeling. *Journal of Emergency Management*, *13*(3), 201–216. doi:10.5055/jem.2015.0234

Sharevski, F. (2015a). Assessing the Quality of Online News Articles as References for an Encyclopaedia Entry. *International Journal of Artificial Intelligence & Applications*, *6*(4), 73–78. doi:10.5121/ijaia.2015.6407

Sharevski, F. (2015b). Cyber Resilience of Software Defined Mobile Networks. In *2015 International Conference on Computing and Network Communications* (pp. 1–6). Trivandrum, India: IEEE. Retrieved from http://www.iiitmk.ac.in/coconet2015/

Sharevski, F. (2015c). Rules or Professional Responsibility in Digital Forensics – A Comparative Analysis. *Journal of Digital Forensics, Security and Law*, *10*(5), 1–12. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/view/287

Sharevski, F. (2015d). The Appropriateness of Factual Density as Informativeness Measure for Online News. In David B. Bracewell (Ed.), *Second InternationalConference on Artificial Intelligence and Applications* (Vol. 34, pp. 99–143). Vienna, Austria: AIRCC.

Sharevski, F. (2016). Cyberattack Surface of the Next-Generation Mobile Networks. In W. Meng (Ed.), *Protecting Mobile Networks and Devices: Challenges and Solutions* (1st ed., pp. 1–17). Boca Raton, FL: CRC Press.