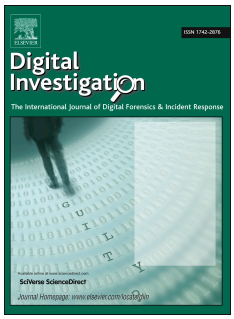
Accepted Manuscript



An analytical analysis of Turkish digital forensics

Mesut Ozel, H. Ibrahim Bulbul, H. Guclu Yavuzcan, Omer Faruk

PII: S1742-2876(17)30388-2

DOI: 10.1016/j.diin.2018.04.001

Reference: DIIN 753

To appear in: *Digital Investigation*

Received Date: 14 December 2017

Revised Date: 5 April 2018

Accepted Date: 6 April 2018

Please cite this article as: Ozel M, Ibrahim Bulbul H, Guclu Yavuzcan H, Faruk O, An analytical analysis of Turkish digital forensics, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.04.001.

An Analytical Analysis of Turkish Digital Forensics

Mesut OZEL mesut.ozel@gazi.edu.tr
H. Ibrahim BULBUL bhalil@gazi.edu.tr
H. Guclu YAVUZCAN gyavuzcan@gazi.edu.tr
Omer Faruk BAY omerbay@gazi.edu.tr

ABSTRACT: The first glimpses of digital forensics (DF) starts back in 1970's, mainly financial frauds, with the widespread use of computers. The evolution of information technologies and their wider use made the digital forensics evolve and flourish. Digital forensics passed a short but complex way of "Ad-Hoc", "Structured" and "Enterprise" phases nearly in four decades. The national readiness of countries might vary for those phases depending on the economy, legislation, adoption level, expertise and other factors. Today digital forensics discipline is one of the major issues of law enforcement (LE), government, defense, industry, academics, justice and other non-governmental organizations as stakeholders have to deal with. We wanted to assess the maturity level of "Turkish Digital Forensics" in view of the digital forensics historical phases, along with some specific institutional & organizational digital forensics issues. The current digital forensic capacity and ability, understanding and adoption level of the discipline, education and training forecasts, current organizational digital forensics framework and infrastructure, expertise, certification and knowledge gained/needed by digital forensics community, tools and SW-HW used in digital forensics, national legislation, policy making and standardization issues along with the anticipated requirements for near future are aimed to address by an online survey. This paper discusses the aforementioned national issues with respect to the digital forensics discipline. It does not examine all aspects of digital forensics. The general assessment we had reached for the maturity level of "National DF" is in between the structured and enterprise phases, with a long way to go but with promising developments.

Key Words: Digital Forensics, Law Enforcement, Survey, Capacity, Ability, Requirements, Policy Making, Standardization, Infrastructure.

1. Introduction

This report focuses on 10 different digital forensics issues that might reveal the current status of Turkish national capacity and readiness via an online survey. The findings may also be interpreted as a basis for other national digital forensics communities, where digital forensics is a new and cross bordered discipline. The survey and the related work is not intended to determine all the aspects of national digital forensics, but to some extend organizational, educational, expertise and process application requirements and along with maturity level assessment of national DF.

National current legislation and billing requirements are not included in this work. It is inevitable for legislation to cope with the continuously accelerating pace of digital technology. Each time interval adds newer digital products (Software- Hardware) which affect the crimes and criminals. The issues that DF has to deal with differ day by day and get wider. The legislation bodies and the relevant stakeholders should follow the developments and act proactively. The main point for legislation is supposed to be not only on defining legal policy and standards, but also on declaring legal methods and uniform national reaction process and procedures.

2. Literature Review

The early digital forensics survey that attempted to add to the growing body of knowledge regarding inherent issues in computer forensics has been conducted in 2004. The study consisted of an Internet-based survey that asked respondents to identify the top five issues in computer forensics. The results indicated that education/training and certification were the most reported issue (18%) and lack of funding was the least reported (4%) by ROGERS and SEIGFRIED [1]. Findings of this work are consistent with the similar and previously declared report for law enforcement community where input from 126 individuals representing 114 agencies sought and 10 critical digital forensics issues named. The issues are; public awareness, data reporting, uniform training and certification, management assistance for onsite electronic crime task forces, updated laws, cooperation with the high-tech industry, special research and publications, management awareness and support, investigative and forensic tools, and structuring a computer crime unit by STAMBAUGH and et al. [2].

Authors evaluated the attitudes and priorities of the Australian forensic community with Delphi methodology in [3]. This work conducted by Brungs and Jamieson, identified 17 legal issues, in 3 categories Judicial, Privacy and Multi-jurisdictional where identification of a set of legal issues facing digital forensics. The top five issues declared in this study were; Jurisdictional, Telecommunications Act Covering Data, Interpretation of Telecommunications Act, International Cooperation in Practice and Revision of Mutual Assistance issues.

Another work by Liles et al. [4], is the extension of Brungs-Jamieson study (The same 17 legal issues) evaluated attitudes and priorities of the U.S. forensic community, in order to determine the importance of the identified issues to five stakeholder groups (Law Enforcement, Academics, Government, Industry, and Legal Experts). The seventeen identified issues for importance ranking in digital forensics are; (1) Jurisdictional (state to state and federal to state), (2) Computer evidence presentation difficulties, (3) Criminal prosecution vs. civil litigation, (4) International