BOOK CHAPTER | "Knowledge is Power"

Device Information for Forensic Analysis

Paul Antwi
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: paul.antwi@st.gimpa.edu.gh
Phone: +233244916336

ABSTRACT

This document provides an overview of information for forensic analysis related to device name, serial number and model of devices used to connect to social networking platforms. The increasing use of social networking applications on smartphones makes these devices a gold mine for forensic researchers. Potential evidence can be captured on these devices and recovered with the right tools and research methods. The increasing proliferation of network devices in homes and buildings increases the possibilities of finding digital traces relevant to an investigation, physical or virtual: cyber-attacks, identity theft, etc. connected to the network can also find useful traces on the devices themselves found or stored in an associated cloud account that can be identified by device ID, model, and serial number.
Keywords: Digital Forensics; Device Information, Evidence, Storage, Cyber forensics framework.

Citation: Paul Antwi (2022): Device Information for Forensic Analysis
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 373-378
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P59

1. INTRODUCTION

In the age of computing, various devices are used along with networking technology for data communication in secured manner. But sometimes these systems are misused by the attackers. Information security with the high efficiency devices, tools are utilized for protecting the communication media and valuable data. In case of any unwanted incidents and security breaches, digital forensics methods and measures are well utilized for detecting the type of attacks, sources of attacks, their purposes.

By utilizing information related to security measures, digital forensics evidence with suitable methodologies, digital forensics researchers detect the cyber-crimes. It is also necessary to prove the cyber-crimes before the law enforcement agency. During this process researchers try to collect different types of information from the digital devices concerned to the cyber-attack. In this process, some key information collected includes device name, serial number of the device and the model of the device.

A serial number is a unique number assigned by the manufacturer to identify an individual device such as a phone, tablet, or laptop. While a device model is the analytical operational framework developed from theoretical and experimental usability studies. This document provides a systematic overview of network connectivity information for forensic analysis related to device name, serial number and model of devices used to connect to antisocial networking platforms.

1.1 Background to the Study

Forensic science is the methodological and correct application of broad spectrum of scientific discipline to answer questions significant to legal system; an interception between technology, methodology and application (Greitzer & Frincke, 2010). The act of establishing a forensic paradigm in digital world involves interpreting digital processes in such a way that it explains 'what' event, action, or process was carried out by or against a particular digital device under examination based on the device ID, device name, serial number, model of the device and among others.

Network forensics has received various definitions since its inception by Marcus J. (Ranum, 2012) and its research community has greatly expanded since then. However, the generally accepted, but not encompassing definition was proposed at the 2001 DFRWS (Palmer, 2001). Palmer (2001), defines network forensics as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities".

Schwartz (2010) describes network forensics as the reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices. In other words, network forensics involves the use of scientifically proven techniques to collect, identify, corroborate, examine, analyze and document digital information from live network session. However, these processes must be in conformance with forensically sound manner. Network forensics evidence source includes the capture of network traffic, and other relevant information from multiple devices, active processes, and digitally transmitting sources. Such device includes audit trails, device name, device ID, model, Logs, routers, firewalls, servers, browsers, honey pot and network security device in general.

Uncovering facts related to planned intent, measurement of success of unauthorized activities, investigation of the source of an intrusion and the reasons for the success of such intrusion as well as the possible reason for such as intrusion are some of the vast needs for network forensics. Additionally, network forensics provides information to assist in response to/or recovery from an intrusion. Thus, network forensics can be termed as proactive, as well as a retrospective approach to both law enforcement, and security hardening perspective. Network forensics can therefore be defined as the act (scientific process) of, measuring level of intrusion; investigating source of intrusion, deciphering intrusion intent and vulnerability exploited; or information provision to recover from an intrusion as well as the process of discovering planned intent of network traffic for the purpose of strengthening system security, and culpable evidence presentation.

Network forensics can be classified into three classes: which are based on purpose, process of collection, and nature of technology used. This paper will look into network connectivity Information for Forensic Analysis in relation to Device name, Serial number and Model of devices used to access social media platform. Social media platform has become popular network platform where diverse devices connect to exchange information.

2. RELATED LITERATURE

Initial work in this area focused on detection techniques and general forensic analysis of smart devices. Burnette discussed the forensics of older BlackBerry versions and the hardware and software used to purchase them (Burnette, 2002). He also described several research methods including the use of hex editors and emulators. Subsequent research provided basic concepts for the forensic analysis of the new smartphone generations such as BlackBerry, Android and iPhone. It outlined the technologies used, the treatment procedures, and the common detection locations for each device based on the device model. Apple devices have been observed to automatically duplicate data in iCloud. It is imperative that Apple users sign in to iCloud before their device can be used. Android devices, on the other hand, do not require Google Cloud for device usage. Therefore, to trace the full location of a data store, a forensic analysis must consider the model of the device.

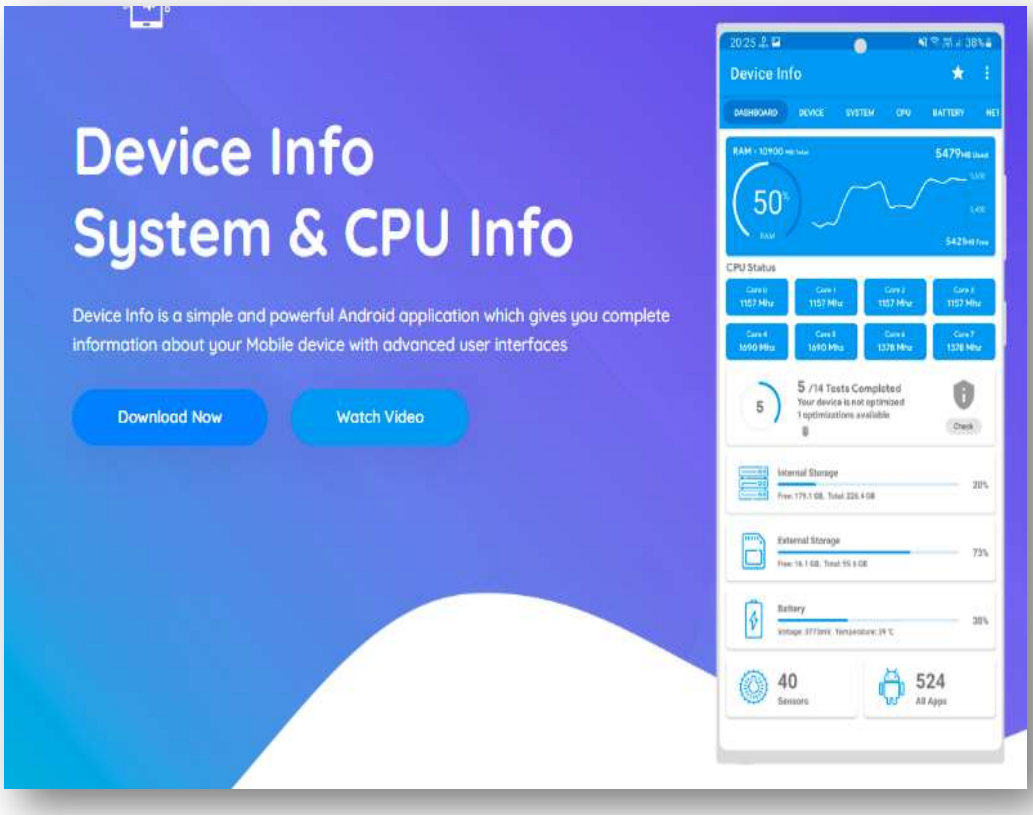

Fig 1: Device Information
Source: https://www.deviceinfo.app/

Punja and Mislan (2008) also reported that device Name and ID are significant piece of network connectivity information which helps forensic analyst to investigate into issues such as cyberbully on the internet especially on social media. The device name and Ip helps to trace the line of communication by extracting data shared two or more internet user: senders and receiver. The data that could be extracted from the internal memory of these devices included call logs, SMS, MMS, emails, webpage bookmarks, photos, videos, and calendar notes (Punja and Mislan, 2008).

Scientific research has also included the investigation of artifacts left by social networking sites on computer systems and tools that assist in the extraction of these artifacts. Zellers has examined the unique data tags and serial numbers created in different MySpace source-code pages and used these tags to create focused artifact keyword searches (Zellers, 2008). While Al Mutawa et al. (2011) research discussed the process of recovering and reconstructing Facebook chat artifacts from a computer's hard disk by the help of the device name, ID and serial numbers. Because many social networking applications are integrated into new smartphones, in cases involving social networks, forensic examiners may be able to find relevant evidence on a suspect's smartphone because every device connected to the internet's registers it identity: Name, ID, Model, and serial number including sources and destination Ips and Gateway address.

A forensic examination of the iPhone 3GS via a logical acquisition showed that a database related to the Facebook application is stored on the phone's memory. The database stores data for each friend in the list, including their names, ID numbers, and phone number (Bader and Baggili, 2010). Two other directories related to the Twitter application were also found. These directories store information about Twitter account data, attachments sent with tweets, user names, and tweets with date and time values (Morrissey, 2010). A forensic examination of an Android phone's logical image showed that basic Facebook friend information is stored in the contacts database (contacts.db) as the device "synchronizes contact's Facebook status updates with the phone book" (Lessard and Kessler, 2010). It also showed that the device stores Twitter passwords and Twitter updates performed through the Twitter application in plain text (Lessard and Kessler, 2010). Forensic research papers on BlackBerry phones and Windows smartphones, however, did not mention finding or recovering any data related to the use of social networking applications.

Similar to computers, smartphones store data that can help determine how the device has been used or misused. Therefore, activities performed through social networks applications may be stored on smartphones. However, previous research has been limited to the recovery of very basic information related to the use of social networking applications. It is clear that further experiments focusing on the recovery of artifacts related to the use of social networking applications are required to determine whether activities performed through these applications are stored and can be recovered from smartphones.

3. RESEARCH GAPS/FINDINGS

The role of forensic network intelligence in the digital age has received commendable attention in criminal investigation versus the collection of physical evidence. From a forensic point of view, the increasing number of networked devices in social media brings opportunities and risks. These devices produce traces that can be useful for investigative and forensic purposes in any type of crime. At the same time, the growth of big data poses challenges for existing digital forensic tools and methods, as large amounts of data can be collected in a short period of time when a device is connected to the network. This makes it difficult for practitioners to extract accurate data without the help of a forensic advisor with specialist knowledge in the field. In addition, these traces can pose challenges for forensic investigators to evaluate and contain vulnerabilities that pose a privacy risk.

4. CONCLUSION

The increasing use of social networking applications on smartphones makes these devices a gold mine for forensic researchers. Potential evidence can be captured on these devices and recovered with the right tools and research methods. The increasing proliferation of network devices in homes and buildings increases the possibilities of finding digital traces relevant to an investigation, physical or virtual: cyber-attacks, identity theft, etc. connected to the network can also find useful traces on the devices themselves found or stored in an associated cloud account that can be identified by device ID or model.

5. RECOMMENDATION FOR POLICY AND PRACTICES

The scope of technology and architecture of network devices has expanded recently, so forensic analysts are advised to pay more attention to the model and type of devices connected to the network, as they are based on a dynamically complex architecture. The way Apple devices access, store, and retrieve data differs from Android and Windows devices.

6. DIRECTION FOR FUTURE

Further research can be carried to investigate into network information forensic on device model and cybercrime relation. The paper can focus on investigative analysis on digital crime and its associated device. A study of this nature will help to identify which model of device cyber attacker recooked useful and intend developed robust forensic tool.

REFERENCE

1. Bader, M. and Baggili, I., 2010. iPhone 3GS forensics: Logical analysis using apple iTunes backup utility.
2. Burnette, M.W., 2002. Forensic Examination of a RIM (BlackBerry) Wireless Device June, 2002. URL https//www. rh-law. com/ediscovery/Blackberry. pdf.
3. Greitzer, F.L. and Frincke, D.A., 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In Insider threats in cyber security (pp. 85-113). Springer, Boston, MA.
4. Lessard, J. and Kessler, G., 2010. Android forensics: Simplifying cell phone examinations.

5. Palmer, B., Walls, M., Burgess, Z. and Stough, C., 2001. Emotional intelligence and effective leadership. Leadership & Organization development journal.
6. Punja, S.G. and Mislan, R.P., 2008. Mobile device analysis. Small scale digital device forensics journal, 2(1), pp.1-16.
7. Said, H., Al Mutawa, N., Al Awadhi, I. and Guimaraes, M., 2011, April. Forensic analysis of private browsing artifacts. In 2011 International Conference on Innovations in Information Technology (pp. 197-202). IEEE.
8. Schwartz, E., 2010. Network packet forensics. In CyberForensics (pp. 85-101). Humana Press, Totowa, NJ.