Digital Investigation 12 (2015) S72–S80

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2015 Europe

Smart TV forensics: Digital traces on televisions

A. Boztas[*], A.R.J. Riethoven, M. Roeloffs

Netherlands Forensic Institute, Laan van Ypenburg 6, The Hague, The Netherlands

Keywords:
Digital forensics
Smart TV
Smart TV forensic
Cyber crime
Digital crime

ABSTRACT

The Smart TV is becoming increasingly popular amongst consumers. Many consumers use a Smart TV to gain quick access to the Internet including video on demand, social networking and instant messaging. Most Smart TVs also provide capabilities to connect with external devices such as a USB flash drive, a mobile phone etc. All of these features make a Smart TV a potentially rich source of information for forensic purposes. With increasing utilisation, it is also easier for malicious users to abuse a Smart TV. Therefore a digital forensics study on the field of Smart TV is imperative. This paper proposes new procedures for acquiring, analysing and investigating a Smart TV.

Introduction

Electronic technology continues to develop. Each day new electronic devices that influence human daily life are entering the market. These devices may store digital data which may be interesting from a digital investigation perspective. A Smart TV (Wikipedia, 2014) is one of these devices. A Smart TV, sometimes referred to as connected TV or hybrid TV, describes a trend of integration of the Internet into television sets and set-top boxes, as well as the technological convergence between computers, television sets and set-top boxes. Smart TVs are available as stand-alone products, but regular televisions can also be made "smart" through set-top boxes that enable advanced functions; for example, Google TV, Apple TV. These devices are mostly IP devices, which enable streaming content over Internet without the need for cable or satellite. Most of the Smart TVs provide access to external hard drives, digital cameras, mobile phones or Internet applications. A Smart TV allows the viewers to connect to the Internet and browse the web as on a computer without the need for additional peripherals. Smart TVs include a wide range of applications which can be used for different means. Viewers can use applications to search and find videos, music, photos and other content on the web, a local cable TV channel, a satellite TV channel or a local storage device.

In the digital forensic area, questions arise as to whether a Smart TV should be an important component of a digital investigation. In the article (Sutherland et al., 2014) a number of questions are posed concerning the relevance of the Smart TV in a digital forensic investigation: do Smart TVs retain and contain relevant information? How easily is this data accessed? In Mutawa et al. (2012) it is stated that the increased use of social networking applications on smartphones makes these devices a "goldmine" for forensic investigators. Is the use of, for example, social networking applications on Smart TVs doing the same for forensic investigators?

This paper presents research on extracting and analysing digital data from a Smart TV in a forensically sound manner. It will give a complete guide to acquiring and investigating data on a Smart TV. This paper does not present an in-depth study of the inner workings of a Smart TV. The scope of this research focuses only on the methods of extracting data from a Smart TV and the global analysis

[*] Corresponding author.
E-mail addresses: a.boztas@holmes.nl (A. Boztas), r.riethoven@holmes.nl (A.R.J. Riethoven), m.roeloffs@holmes.nl (M. Roeloffs).

http://dx.doi.org/10.1016/j.diin.2015.01.012

of the said acquired data. Our goal is to show that a Smart TV may indeed contain different kinds of digital traces which can be relevant for investigations, such as, pictures, connected devices, visited websites, etc. If forensic examiners are not knowledgeable regarding the different types of Smart TV based systems and what artifacts each may leave behind, they could miss critical information during an investigation.

Related work

Earlier work on Smart TVs focuses mainly on gaining access to the Smart TV in order to get user data remotely (Grattafiori and Yavor, 2013) and (Lee and Kim, 2013). The latter authors also go further into making a surveillance device from the Smart TV, by recording audio and video from the built-in microphone and camera respectively. The main point made in the previous research is that it is not that hard to find ways to gain access to the Smart TV on a low-level. With these methods it should be possible to gain access to a Smart TV. There is no forensic research available for any brand or model of Smart TV.

From a hardware perspective, the Smart TV is just an embedded system with a large (for example 40-inch) screen. The Smart TV can be handled like any embedded system. An embedded system which has been investigated thoroughly is a mobile phone. Willassen (2005) and van der Knijff (2010) show methods which can be used during the investigation of a Smart TV.

Materials and methods

In this section we will explain how we carried out this research. Initially, a literature and market share survey was conducted. The Smart TV market continues to grow (Tarr, 2013) and expand rapidly in major countries (Hong, 2013). We determined which models and brands of Smart TV are popular (Top10, 2014) or more common under users and which functionality of these Smart TVs are commonly used. On the basis of this literature study, the model and type of the Smart TV for our research was selected. Secondly, we set up an experimental environment to generate different types of digital traces when using the Smart TV. Finally methods were developed to acquire and analyse the digital traces of this Smart TV.

Selecting a smart TV

As previously stated, there exists a great deal of variety of types and models of Smart TVs on the market. The features available on a Smart TV vary depending on the brand and model of TV. Most Smart TVs will allow access to popular social networking sites and communication programs such as Skype. The most popular brands of Smart TV are Samsung, LG, Panasonic and Sony. This research was conducted on a Samsung television model UE40F7000SLXXN, based on popularity, the fact that it contains a camera and microphone, and the fact that Samsung has an open source platform for their Smart TVs. The Samsung Smart TVs are very popular amongst customers and offer a great deal of functionality which therefore may leave relevant digital traces for a digital investigation. This type of television allows the viewer to install applications, visit websites, peruse pictures, communicate by voice and video, connect external devices, etc. User data was generated by performing different usage scenario's which covered most of the available functionality of the Samsung Smart TV.

Data acquisition methods

The selected Smart TV uses flash memory as storage. The flash memory on the investigated Smart TV is an eMMC chip (Wikipedia MultiMediaCard, 2015). Depending on the hardware, there are several options to acquire data. The following methods for acquiring the data were utilised:

- eMMC five-wire method: an eMMC chip, like the one used in our reference Smart TV only needs five signals to be connected: Vss, Vdd, Clock, Command & Data0. These signals were detected on the main board. It is then possible to read the eMMC chip using a standard USB SD-cardreader attached to a writeblocker.
- NFI Memory Toolkit II (MTK II): (NFI, 2011) this is a universal forensic solution that enables investigators to read memory chips and potentially extract user data – such as text messages, phone numbers, pictures and browser history – from a wide variety of devices. The MTK II is a combination of hardware and software. The hardware makes a physical connection, generates signals and supplies power to a memory chip, while the software runs the necessary command-sets to access data in the various types of memory chips.
- Application: a software approach for acquiring data is the use of a custom application with a small footprint which was installed on the Smart TV and writes the data out to an external storage device. This might be possible as Samsung distributes a Software Development Kit to develop applications for this particular model of Smart TV.

Analysis of digital traces

The fundamental goal of this research is to determine which digital traces are left behind on a Smart TV for investigation purposes. This means that this paper is not a complete description of the inner workings of this particular Smart TV and instead is focused on acquiring traces of user interaction. Different tools and forensic programs like EnCase were used to search through the data of the Smart TV. Our research was focused on the following types of traces which may well be relevant for a digital forensic study:

- System information and settings: device name, connected devices, network information and smart functions.
- Apps: Facebook, Twitter, YouTube, etc.
- Web browsing: visited websites, traces of search engines, etc.
- Photo and multimedia files