Video surveillance: The forensically sound retrieval and investigation of picture content off a memory dump

Stefan Kiltz, Tobias Hoppe, Jana Dittmann, Claus Vielhauer

Otto-von-Guericke University of Magdeburg,
Department of Computer Science
Universitaetsplatz 2
39106 Magdeburg, Germany
{stefan.kiltz, tobias.hoppe, jana.dittmann, claus.vielhauer}@iti.cs.uni-magdeburg.de

In this paper we cover the process of securing digital evidence contained in the main memory of IT-systems. This is done on a practical scenario where the digital evidence is represented by pictures produced by a camera surveillance application running on a Windows-based system Illustrated by the results from this practical setup, we give an extended guideline about how to forensically acquire, locate and extract graphics content within memory dumps of Windows-based systems.

The entire application is based on a forensic model presented in [KHD09] and illustrates central aspects of the model by means of this practical application scenario. This includes the assurance of integrity and authenticity of evidence gathered this way using cryptographic mechanisms.

Two different means of gathering the digital evidence are outlined and combined into an application. It also implements the securing of the evidence data against unauthorised manipulation starting with the creation of the memory dumps. This is done by means of integrity hashing as well as authenticity provision in one atomic step, thus ensuring forensic soundness.

With respect to the evaluation of the evidence gathered this way, general approaches of the identification of image data contained in the raw dump files are introduced. Starting with the demonstration of manual approaches, also a first approach towards the automated extraction of the graphics content is presented, based on the picture content characteristics. To proof data authenticity, unique hardware identification data can be extracted off the memory dump, thus linking the extracted picture content to a particular processing hardware.

The advantage of our proposed approach we see in handing the initiation of the data gathering process over to the operator of an IT-system whilst still allowing for a forensic sound investigation. With our approach the picture content is effectively tied to the application and the IT-system that runs it, ruling out most claims of manipulation of the resulting picture.