Unified Forensic Methodology for the Analysis of Embedded Systems

R.J. Shaw, A.S. Atkins
Faculty of Computing, Engineering, and Technology, Staffordshire University, Beaconside, Stafford, UK
e-mail: r.shaw@staffs.ac.uk, a.s.atkins@staffs.ac.uk

Abstract – Embedded systems are ubiquitous in society and can contain information that could be used in criminal cases for example in a serious road traffic accident where the car management systems could provide vital forensic information concerning the engine speed etc. A critical review of a number of methods and procedures for the analysis of embedded systems were compared against a 'standard' methodology for use in a Forensic Computing Investigation. A Unified Forensic Methodology (UFM) has been developed that is forensically sound and capable of dealing with the analysis of a wide variety of Embedded Systems.

I. INTRODUCTION

Whilst there is no defined standard for the analysis of a PC during an investigation, there are a number of 'rules' that any investigation must follow. Embedded systems are pervasive and whilst it is impossible to create a definitive list of where they are used, examples of embedded systems can be found in every walk of life, from office systems, production systems, household equipment, games consoles, car management systems, event data recorders, mobile phones and satellite navigation etc.

An embedded system can be viewed as a computer system, that cannot be programmed by the user, that is designed to perform a few dedicated functions. When analysing a computer or similar device, this is usually undertaken by the removal of the hard disk, and then taking a bit-by-bit copy, or image. Any analysis is then performed on the image, ensuring that the original evidence remains unaltered

With embedded systems, the removal of data from the storage device may prove complex and the investigator runs the risk of altering or even destroying evidence [1]. It is important to realise that within Embedded Systems, any evidence/data is usually stored not in a within a hard drive but in a memory store built into the Embedded System.

Embedded systems that are used for such things as high performance vehicle management, aircraft control and transportation control (rail/sea/air) i.e. those systems that are not in the public domain or available for public use (for example black boxes from aircraft incident investigation), have special procedures for the retrieval and analysis which are outside the scope of this paper.

As with any evidence collection, there are a few basic rules that must be adhered to. Firstly, it is vital that any data collected is not modified in any way, or if modification is unavoidable, the nature/type and amount of modification is known and understood. Secondly, it is important that the artefact (embedded system) itself be subjected to a set of controls that ensure the custody chain is documented. Thirdly, the whole process of collecting and analysing the data/evidence must be documented to ensure that no steps are 'missed' and that the process is repeatable. With these general rules/steps in place, the analysis of an embedded system (indeed any system embedded or otherwise) can be seen to be acceptable within a legal environment.

It should also be realised that there is likely to be data relevant to the investigation that is not stored directly on the embedded system, but in components surrounding or linked to it – so called 'neighbourhood data'.

Given the ongoing expansion of technology into all facets of society, and the development of new ways to leverage existing technology, it is not feasible to develop a methodology that will encompass every single type of embedded system for forensic analysis. The intention of the paper is to outline a generic methodology that can be used to cover existing and new embedded systems.

In recovering data from an embedded system, it is possible that the module holding the data, will need to be removed from the equipment that it is attached to for example an event recorder from a car following a crash etc. In this situation the chain of custody must be started, and the item protected from inadvertent or deliberate modification. Once the data store is available for analysis then it is likely that an external power source will be

required to access the data. This is likely to result in modification of the data and therefore all data collection connections should be made before power is applied to the device under investigation. Alternatively, power may need to be provided to the device during its removal to ensure no loss of power and therefore data

II. EXAMPLES OF EMBEDDED SYSTEMS

A. Event Data Recorders

Event Data Recorder's (EDR's) as indicated in Figure 1 are used to record and preserve the current state and configuration of the item under investigation, at the moment when some critical event occurs. For example a car accident, where such things as speed, air-bag deployment etc will be recorded, or more sophisticated 'Black box' recorders on aircraft, that will record speed, altitude, control lever and dial settings and cockpit voices.

Figure 1 Sensing Diagnostic Module Housing an Event Data Recorder [2]

EDR's are most commonly used in transport vehicles to identify specific events such as accidents, rather than 'long term' ongoing data recording. Long term recording with EDR's can be undertaken, but tend to be restricted to testing and evaluation of high value machinery for example performance monitoring of Formula 1 racing car, where data is recorded on an ongoing real-time basis.

Different EDR's have different capabilities in what they store. Most passenger vehicle EDR's have the capability of recording the measured deceleration from the crash and such things as air bag deployment. Other systems can store up to five seconds of pre-crash data including vehicle speed, engine RPM's and percent throttle etc.

B. Game consoles

Game consoles are essentially modified computer systems that have been specifically developed to run home video games as illustrated in Figure 2. As with most computer systems, they consist of a data storage device, processing capability but with enhanced video/graphics capability and modified I/O devices – usually hand held controllers, some with motion sensors. Access to the data storage device is fairly straight forward, but some systems are known to use encryption.

Figure 2 Game console Xbox 360

C. Satellite Navigation Systems

Satellite Navigation (Sat Nav) devices are mobile devices that are able to determine their location on using the position of orbital satellites. They are used to plan routes to specific destinations, either directly or via specific waypoints, from a particular origin, typically the user's home as shown in Figure 3. A Sat Nav stores details of journeys, times and dates the journey was plotted and the recovery. Analysis of this data can be used as evidence as part of a criminal investigation and are commonly found in vehicles and marine craft.

Figure 3 Satellite Navigation System

III. CURRENT METHODS AND PROCEDURES FOR EMBEDDED SYSTEMS ANALYSIS

There are several methods and procedures that are currently available for the investigation of embedded systems which are outlined as follows:

A. Van der Knijff

Van der Knijff [3] proposes a set of selection criteria that will assist with the collection and analysis of data. These include identifying relevant data that is linked to an individual, `ensuring methods and techniques used are as universal as possible, obtaining help from the relevant industry as required and checking the possibility of using methods and techniques that do not require any

previous or expert knowledge. The process proposes a series of ten steps in the recovery and analysis of embedded data. This begins with a preservation step, proposes the repair of any damaged embedded system, through data recovery stages, through to analysis and reporting. It also specifies the recovery of Neighbourhood Data.

B. Harris et al

Harris et al [4] have a set of protocols that relate directly to the recovery and investigation of Event Data Recorders (EDR's) Preliminary steps are to photograph the vehicle to give assistance to data interpretation (such as air bags being deployed, transmission type etc). There are then a series of steps, grouped together in four stages. These stages are *Data Retrieval*, where data is captured from the EDR, *Securing Recovered Data*, where the recovered data is copied to a removable computer hard disk – the reference disk, *Data Recovery Records*, where details such as how & when the data has been recovered, the initial state of the evidence, etc, are logged and finally *Data Presentation*, how data is presented or explained to a jury or investigative panel.

C. Kyung-Soo and Sangjin

This methodology [5] consists of two separate phases within which are a number of specific steps. There is a *Hardware Analysis Phase*, which analyses the hardware of the Embedded System to determine make, model, configuration etc and a *Software Analysis Phase* that recovers the system configuration, file listing, file analysis etc.

D. Carrier & Spafford

Carrier and Spafford [6] have developed a process model for general digital investigation. This model consists of a total of five phases, *Readiness*, to ensure that the investigator/team is ready & capable to handle the investigation *Deployment*, to ensure that all notifications authorizations have been obtained and agreed, a *Physical Investigation* and *Digital Investigation* phase – where the hardware and software/data associated with the investigation are acquired and analysed, and a *Review* phase to ensure that, post investigation, all steps were completed correctly - with each main stage being subdivided into specific stages of the investigation.

E. Beebe and Clarke

Beebe & Clarke [7] have proposed a six phases, objective based approach, based upon a number of different models and frameworks. These are *Preparation*, to ensure the readiness and capability of the investigator(s) *Incident Response*, where the stages and processes to be followed are planned and agreed *Data Collection*, where the evidence is collected, *Data Analysis*, where the evidence gathered is analysed, *Findings Presentation*, to present the results of the investigation *to relevant bodies*, and *Incident Closure*, where the stages and process followed are reviewed. This objective based approach is perceived as a better approach since each "criminal event" will be different.

F. PDA Forensics - Paraben

The use of Paraben software [8] in PDA forensic analysis is well known and has become a de facto standard. There is a standard method used with the software package that can be modified dependent upon the type of hardware being analysed, PDA, Blackberry or Windows based device. This is a three stage process, namely *Seizure*, where the PDA is obtained, *Acquisition* where the e-evidence is extracted from the PDA and *Analysis*, where the data obtained is analysed in relation to the investigation.

G. CCIPS Digital Forensics Analysis Methodology

The Cybercrime Lab in the Computer Crime and Intellectual Section (CCIPS) has released a flow chart showing how they would approach a digital forensic case [9] as shown in Figure 4. The CCIPS name seven stages, namely *Obtaining & Imaging Forensic Data*, *Forensic Request*, *Preparation/Extraction*, *Identification*, *Analysis*, *Forensic Reporting*, and *Case Level Analysis* which they believe should be completed by an investigator for an examination of evidence to be successful. The CCIPS focus on three stages in particular *Preparation/Extraction*, where the evidence gathering systems are prepared, and data is extracted from the device, *Identification* where the evidentiary "relevance" of the data is determined, and *Analysis* where the specific data relating to each item of evidence is noted.

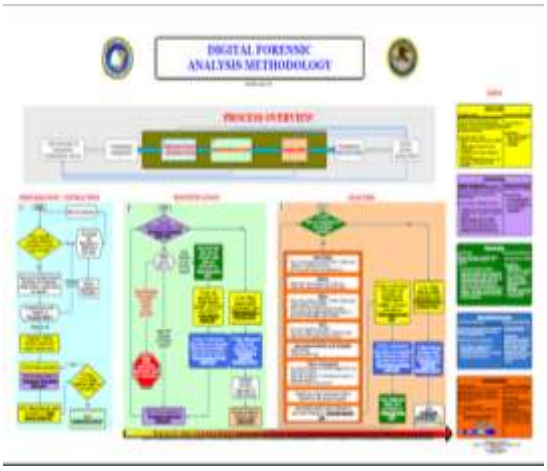

Figure 4 CCIPS Digital Forensic Analysis Methodology

	Van der Knijff	Harris et al	Kyung-Soo & Sangjin	Carrier & Spafford	Beebe & Clarke	PDA (Paraben)	CCIPS [Benchmark]
PREPARATION PHASE				**Readiness Step** - Operations - Infrastructure **Deployment Step** - Detection & Notification - Confirmation & Authorization	**Preparation Step** - Planning - Training etc **Incident response** Pre-investigation response to -detect -assess -validate -determine a response strategy		**Preparation Step** Setup and validate forensic hardware and software; create system configuration as needed.
HARDWARE PHASE						**Step 1 – Seizure** Seize PDA	
	Step 1 - Preservation Step 2 - Repair			Preservation step		Replace batteries, or plug-in device to power supply	
				Survey Step - "Walk through" of crime scene Documentation step			
				Search & collection		Seize PDA cradle and connection cables	
				Reconstruction			
	Step 3 - Determination of Type		**Hardware Analysis Step** -Check product name & version -Check hardware specification -Check hardware modification -Compare storage device settings -Check storage configuration				
				Presentation			

	Van der Knijff)	Harris et al	Kyung-Soo & Sangjin	Carrier & Spafford	Beebe & Clarke	PDA (Paraben)	CCIPS [Benchmark]
SOFTWARE PHASE				Preservation			
				Survey			
				Documentation			
	Step 4 - Device Data Inquiry	Data retrieval		Search & collection	Data collection	**Step 2 - Acquisition** – dependant on PDA type	Obtaining & Imaging Forensic Data
	Step 5 - Neighbourhood Data Inquiry	Securing Recovered Data				Memory acquisition	
	Step 6 - Device Data Recovery					File acquisition	
	Step 7 - Neighbourhood Data Recovery					Database acquisition	
						Registry acquisition	
							Forensic Request
				Reconstruction			Preparation/Extraction (Of Evidence)
	Step 8 - Analysis of Data		Software Analysis		Data analysis	**Step 3 – Analysis** Palm Device Blackberry Windows device	Identification (Pre-analysis)
			Check product name & version				Analysis
			Compare system configuration				
			Check directory configuration				
			Check file list				
			Mission specific file analysis				
			Log file analysis				
			Check metadata related to MAC time				
			Timeline analysis				
			Correlation analysis				
	Step 9 - Reporting the Findings			Presentation	Findings presentation		Forensic Reporting
	Step 10 - Audit Trail	Data Recovery Records		Review	Incident closure		Case Level Analysis
		Data Presentation					

Table 1 Comparison of six methodologies to the CCIPS methodology [Benchmark]

IV. RESULTS

A review of digital forensic analysis has highlighted a total of six methodologies that are applicable to the forensic analysis of embedded systems. These have been compared against the CCIPS [9] forensic digital methodology, to identify similarities and omissions. Using this information a proposed generic system, the Unified Forensic Model (UFM) following the recognised CCIPS model as the 'spine' and supplementing with best practice from the others has been developed.

From a series of iterations of analysing the tabulated results of the six different methodologies, it became apparent that in the overall investigation process, there are three distinct phases, namely a **Preparation Phase**, **Hardware Phase** and **Software Phase.** Each phase is subdivided into steps, with a matching colour code being used to identify matching analysis steps.

Table 1 shows the individual methodologies coupled with a colour coded system to highlight the comparison stage of this investigation. For example, in the Hardware Phase the preservation is colour light green to signify a direct comparison of the naming convention i.e. *Preservation* is named in both the Van der Knijff and Carrier & Spafford. As you move down Table 1, i.e. through each methodology, the colours are again chosen to reflect similarity between steps, in that they each cover the same concept of the investigation step, e.g. the *Search & Collect* step in Carrier & Spafford compares with the S*eize PDA* step within the Paraben methodology.

Evaluating the colour coding displayed in Table 1, a number of similarities become apparent. Only two methodologies (Carrier & Spafford and Beebe & Clarke) had any pre-investigation steps. In a forensic investigation an investigator may be required to analyse a variety of embedded systems. The Preparation Phase is extremely important to ensure that both the investigator, and the laboratory/equipment used, is capable and ready for use. This will ensure that an adequate amount of training and familiarisation has been undertaken, that the appropriate equipment and specialist tools are available and that the correct legal and documentary procedures have been adhered to prior to the investigation.

In phase 2, the Hardware Phase, all of the methodologies being evaluated, except Harris and Beebe & Clarke have some form of hardware analysis. Interestingly, the CCIPS methodology used as a benchmark also does not include a Hardware Phase. Only the Carrier & Spafford methodology contained a documentation step within the Hardware Phase. In general, there was similarity between the Van der Knijff, Kyung-Soo & Sangjin, Carrier & Spafford and Paraben PDA methodologies where any hardware analysis was present. The Hardware Phase directs the investigation solely towards the preservation, analysis and investigation of hardware associated with the case, be it the hardware that electronic data will be extracted from, or hardware that is merely "associated" with the items under investigation.

As all of these methodologies are designed around electronic investigation and analysis, it would be expected that all of the methodologies have some form of software/data analysis phase within them. Table 1 depicts the Software Phase and identifies the different steps within each methodology. This compares favourably with the benchmark CCIPS methodology. The most salient point of the Software Phase depicted in Table 1 is that all of the methodologies have a presentation step, with the exception of Kyung-Soo & Sangjin and Beebe & Clarke. It is unusual to find no presentation step within a methodology in terms of any Forensic Investigation. Table 1 indicates that only the Carrier & Spafford methodology covers all three phases. However, there are no software analysis steps within this methodology.

Figure 5 shows a proposed Unified Forensic Methodology for Embedded Systems Analysis (UFM-ESA) which indicates the three distinct phases of Preparation, Hardware and Software. Within each Phase is depicted the separate and specific steps that are required for the forensic analysis of an Embedded System.

This proposed methodology, whilst based upon the standard CCIPS methodology, also includes a Hardware stage which appears not to be specifically inferred within the CCIPS Methodology. The UFM-ESA Methodology is based upon the strengths of each reviewed methodology, using the CCIPS methodology as a benchmark, to ensure that there is a standard methodology for the analysis of embedded systems. Further work will be carried using this methodology to validate the proposed steps within each Phase of the methodology, using case study and physical embedded systems to provide a comprehensive procedural guide to assist practitioners in the investigation of Embedded Systems.

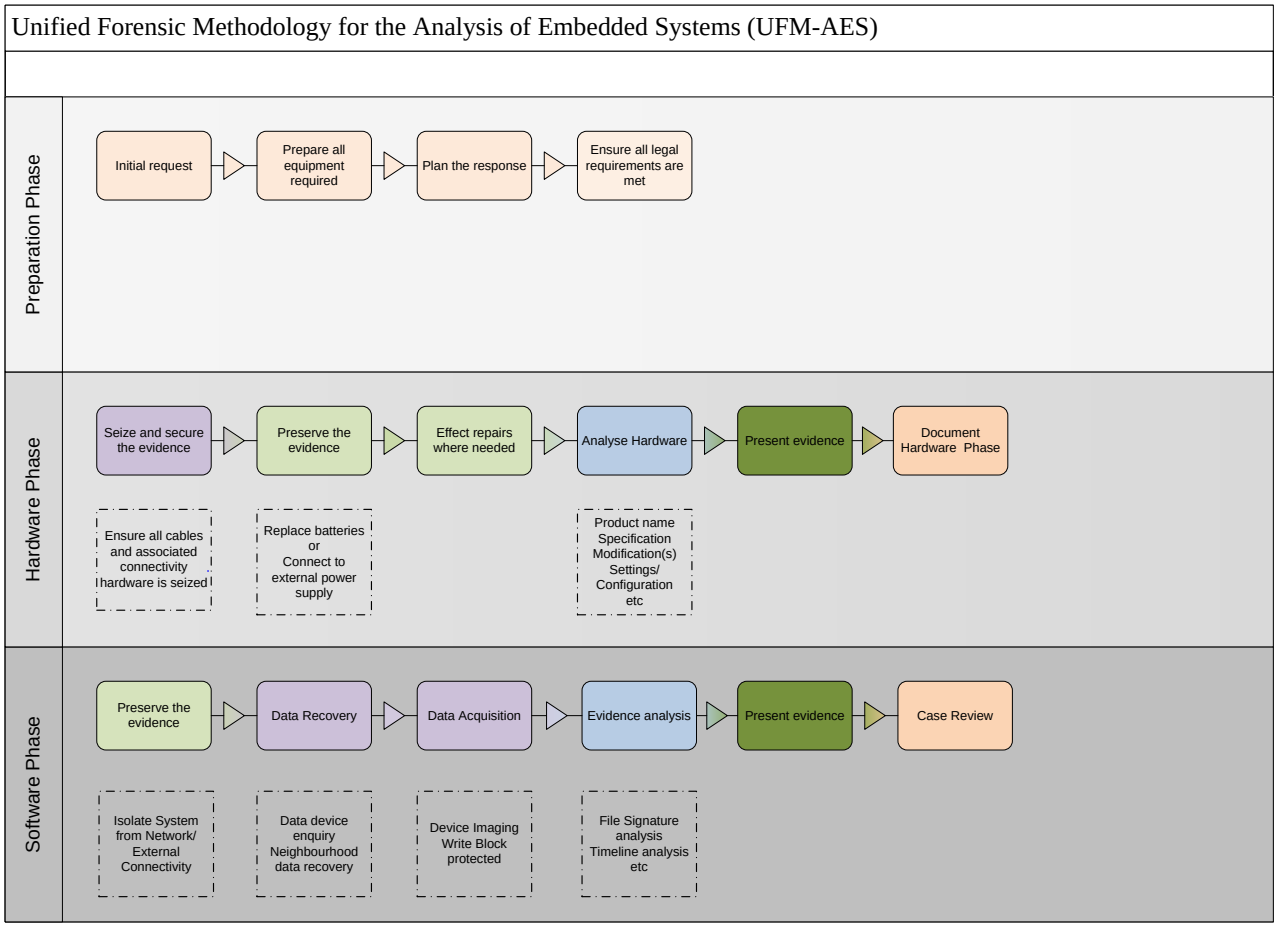

Figure 5 Proposed UFM-AES Methodology for analysing Embedded Systems

V. CONCLUSION

The paper outlines a review of six methodologies that appear to be relevant to the analysis of embedded systems. The methodologies were analysed in terms of three main phases**, Preparation, Hardware** and **Software** and a colour coded analysis was produced to allow for a comparison which is depicted in Table 1. The CCIPS methodology was used as a benchmark to assist in the analysis.

The analysis indicated that the Carrier & Spafford covered each of the three phases; however, there are no software analysis steps within this methodology. Further, whilst the CCIPS methodology has been used as a benchmark, a Hardware stage appears not to be specifically inferred within the CCIPS Methodology

The paper outlines a proposed Unified Forensic Methodology for the Analysis of Embedded Systems (UFM-AES). The methodology is based on the analysis based on the analysis outlined in the paper of six separate investigation methodologies. This UFM-AES will now provide a standard methodology for the analysis of embedded systems. Further work is being undertaken to produce a set of more detailed procedural guidelines to assist an investigator in the Forensic Analysis of Embedded Systems.

References

[1] Glennon, J. G., http://www.crashforensics-.com/automobiledatarecorders.cfm [Accessed: 01/09/10]

[2] GM General Motors http://www.gm.com/-corporate/responsibility/safety/event_data_recorders/ [Accessed: 01/09/10]

[3] Van der Knijff, R. M. (2002). Embedded Systems Analysis. Chapter 11 of Handbook of Computer Crime Investigations - Forensic Tools and Technology. 2002. Academic press

[4] Harris, J. O, Wilson W. C., Badger J. E. (Ed) http://www.harristechnical.com/articles/mvedr.pdf [Accessed: 10/05/2010]

[5] Kyung-Soo L., Sangjin L., "*A Methodology for Forensic Analysis of Embedded Systems*", Future Generation Communication and Networking, vol. 2, pp. 283-286, 2008. Second International Conference on Future Generation Communication and Networking, 2008.

[6] Carrier, B., Spafford E., "*Getting Physical with the Digital Investigation Process*", International Journal of Digital Evidence, Volume 2, Issue 2, Fall 2003

[7] Beebe N. L., Clark, J. G., "*A hierarchical, objectives-based framework for the digital investigations process*", Digital Investigation, Volume 2, Issue 2, June 2005, Pages 147-167.

[8] Paraben http://www.paraben.com

[9] CCIPS, 2007 Cybercrime Lab in the Computer Crime and Intellectual Section. (2007). *Digital Forensic Analysis Methodology.* [Online]. 22nd August 2007. Available from: http://www.justice.gov/criminal/cybercrime/forensics_chart.pdf . [Accessed: 10/03/2010]