Survey of Evidence and Forensic Tool Usage in Digital Investigations

AER Specification Result
Final Report for the SFI STTF Grant
07/RFP/CMSF575 STTF 09

Joshua I. James

Introduction

This report has been created to fulfill requirements set forth in the Science Foundation Ireland, Short Term Travel Fellowship Grant (*07/RFP/CMSF575 STTF 09)* for the **Reseach into real-world digital forensic practices for the development of highly automated tools to increase speed and efficiency of forensic investigations** project.

This document will report on the state of the established objectives of the project:

1. Acquire knowledge of the business process of an investigation through observation, legal needs review, and interviews with practicing investigators
2. Gather investigator requirements for digital forensic tools
3. Evaluate results obtained
4. Generate a specification for a useful forensic tool using AER algorithms

1. Knowledge Acquisition

After spending the project period with INTERPOL's Financial and High-Tech Crime Sub Directorate, I was able to gain insight into how INTERPOL functions from within and their strategy to stop international crime. The key information learned:

- Every country has a different *definition* of digital crime
- Every country has different *laws* relating to digital crime
- INTERPOL fights international crime by managing resources between countries
- INTERPOL provides facilitation rather than direct operational capabilities
    - 'Outsource' operational needs from member countries

2. Gather Requirements for Digital Forensic Tools

INTERPOL's strength is its vast network. This network was used to distribute a very brief survey to practicing digital investigators. Out of 30 surveys submitted, 10 were returned. The result of this survey is given in **Appendix A**. Along with these surveys, informal discussions with practitioners were conducted. The results are evaluated in section 3.

3. Evaluate Results

Through the survey and discussions there are several primary factors investigators take into account when purchasing forensic software such as:

1. Feature set
2. Cost
3. Ease of use

Cost is a common complaint, and a major concern for almost every practitioner spoken to. However, the most expensive forensic software, Encase, was the primary software chosen by 80% of the organizations. FTK, X-Ways Forensic, and miscellaneous tools were also used, but not nearly as often.

The average percentage of cases in which *only* the chosen primary software was used is 77.9%. Which seems to denote that the cost of more expensive software is justified if it can handle the majority of needs the investigator may have. It appears that Encase does, in fact, meet the majority of requirements of the investigator, however, there is still approximately 20% of the cases in which an investigator would need additional features.

This 20% is covered by various secondary software, with FTK being the secondary software of choice. WinHex, Password Recovery/Decryption, Automated Analysis tools, and various Linux-based tools were also used.

The majority of the time an investigator is looking at user documents with Internet, passwords and log analysis a close second.

The group also indicated that they would be more likely to buy a plug-in to their current software-set than to buy a third-party stand alone software. Fitting into their current workflow is a topic of importance.

Timelines of user actions are important to investigators, however, determining exactly how often they would be use cannot be determined due to ambiguous wording of the question. Some investigators indicated that a timeline of user activities would be useful in up to 70% of their cases.

Also interesting is that currently only 31% of cases involve Windows Registry Analysis. This low number was **not** shown to correlate with knowledge of the Windows Registry. Responders who claimed to be “very familiar” or “expert” in Windows Registry analysis, employed it just as often as those who were only “somewhat familiar”.

Finally the types of evidence investigators are seeing still consist primarily of Windows computers (87%) with Linux a far second (7%) and Mac last (6%). Of the

Windows machines, Windows XP is still the most common OS (58%) with Vista (28%) and Windows 7 (4%) growing, but still not the majority.

4. Generate Specification for Useful Forensic Tools

Based on the information collected by both discussion and surveys, a preliminary software requirement specification will be created.

a. **Functionality**
    i. The function of the product is to automate evidence reconstruction using methods developed in the AER project
        - Primary analysis target: Windows XP, Vista and Windows 7
        - Secondary analysis target: Linux systems – Low priority
        - Tertiary analysis target: Mac OS – Low priority
    ii. The product must automate common digital evidence analysis tasks
    iii. The product must focus on user documents, user actions, and logs
    iv. The product must improve analysis quality and time
        - Time to manually conduct an equivalent analysis by a knowledgeable practitioner will be used to measure performance
    v. The product should include a timeline view of user events
b. **Interface**
    i. The product must be intuitive, as in it should be obvious even to people with little-to-no training how to use each of the features.
    ii. The product should integrate into Encase and FTK as a "plug-in"
        - The product should integrate into the investigator's work flow
        - The product must not impede any other function of the software
c. **Performance**
    i. The product should focus on speed of analysis
    ii. Each algorithm should compliment each other to avoid redundant processing
    iii. The product should not affect the speed or function of any other analysis software
d. **Attributes**
    i. The product must be verifiable, and tested to be correct
    ii. The product, or algorithms should port to Linux
e. **Design Constraints**
    i. The product must run on Windows Systems (XP, Vista, Windows 7)
    ii. The product must be in English

Appendix

Appendix A: Survey Data

Survey data from which this document was created can be found in "SFI STTF – Report Survey Data.xls"

Surveys	Replies	Reply %
30	10	33.333

Primary Software (Some listed more than one)

Encase	8
FTK	4
X-Ways	3
Other	3

% of Time only Primary Software Would Be Used

40	
80	
90	
90	
99	
70	
90	
90	
80	
50	
77.9	**Avg.**

Other Software (Some listed more than one)

FTK	5
Image ID	1
FOCA	1
WinHex	3
Xways	1
Tracehunter	1
NetAnalysis	1
Password Decryption	2
Virtualization	1
PC3000	1

Other	5
COFEE	1

What types of information is normally looked for?

Multimedia	1
Communication	1
Documents	2
Log Analysis	1
Internet	1
Live System Activity	1
Mail Recovery	1
Passwords	1

Would you be more likely to use a 3rd party tool if it were a plug-in to your main software?

yes	7	
no	0	
maybe	1	(depends on price)

Approx. how many cases per month would a timeline of user activities be useful?

4
3
20
5
most
15
70%
5

What % of cases involves Windows Registry Analysis?

20	
20	
50	
10	
100	
10	
25	
10	
30.625	**Avg.**

How familiar are investigators in your organization with the Windows Registry?

3		
3		
2		
2		
3		
2		
2		
2		
2		
2.333	**Avg.**	(Somewhat Familiar) Basic Knowledge Level

Suspect Operating Systems

Windows		Mac		Linux	
	80		18		2
	90		1		9
	65		5		30
	85		10		5
	95		0		5
	95		3		2
	90		7		3
	99.9		0.05		0.05
	80		10		10
	90		3		7
Avg.	**86.99**		**5.705**		**7.305**

Windows Breakdown

2000	**xp**	**vista**	**7**	**95**	**98**	**ME**	**NT**
20	60	10	10	0	0	0	0
3	85	0	0	1	7	2	2
0	45	55	0	0	0	0	0
10	45	35	5	0	2	2	1
15	60	20	5	0	0	0	0
5	75	5	0	0	0	0	0
0	45	55	5	0	0	0	0
2	60	35	2	0.5	0.5	0	0
0	50	40	7	0	1	0	2
6	**58**	**28**	**4**	**0**	**1**	**0**	**1**