

Open Source Software For Digital Forensics

[DOWNLOAD HERE](#)

1;Chapter 1;8 1.1;The Case for Open Source Software in Digital Forensics;8 1.1.1;1.1 Introduction;8 1.1.2;1.2 Definitions;9 1.1.3;1.3 Making the Case for Open Source Software;9 1.1.4;1.4 Conclusions;11 1.2;References;12 2;Chapter 2;13 2.1;Computer Forensics Education the Open Source Approach;13 2.1.1;2.1 Introduction;13 2.1.2;2.2 Computer Forensics Software Tools;15 2.1.3;2.3 Case Study;16 2.1.3.1;2.3.1 Computer Forensics Workshop - Content and Outcomes;17 2.1.3.2;2.3.2 Workshop Requirements;18 2.1.3.3;2.3.3 Laboratory Structure;19 2.1.3.3.1;2.3.3.1 FAT File System Investigation;19 2.1.3.3.2;2.3.3.2 Ext File System Investigation;20 2.1.3.3.3;2.3.3.3 NTFS File System Investigation;20 2.1.3.3.4;2.3.3.4 Media Preparation and Imaging;21 2.1.3.3.5;2.3.3.5 Network Forensics Modules;21 2.1.3.3.5.1;Network Activity Reconstruction;21 2.1.3.3.5.2;Web Browsing Activity Reconstruction;21 2.1.3.3.5.3;Email Extraction and Reconstruction;22 2.1.3.3.6;2.3.3.6 Applied Cryptography Modules;22 2.1.3.3.7;2.3.3.7 Live System Analysis;23 2.1.4;2.4 Commercial Software Alternative;24 2.1.5;2.5 Conclusions and Future Work;25 2.2;References;26 3;Chapter 3Virtual Machine for Computer Forensics the Open Source Perspective;28 3.1;3.1 Introduction;28 3.2;3.2 Overview of Virtualisation Methods;29 3.3;3.3 Virtual Environments in Computer Forensics Investigations;32 3.3.1;3.3.1 Booting Acquired Disk Image in Virtual Environment to Recreate Investigated Computer;34 3.3.2;3.2 Accessing Disk Images From Different Operating Systems;36 3.3.3;3.3.3 Shifting of Computer Forensics Environment From Windows to Linux;37 3.4;3.4 openSUSE And Other Linux Distributions;37 3.4.1;3.4.1 openSUSE and VirtualBox;38 3.4.2;3.4.2 openSUSE and Xen;40 3.5;3.5 Conclusions and Future Work;43 3.6;References;44 4;Chapter 4;47 4.1;Open Computer Forensic Architecture a Way to Process Terabytes of Forensic Disk Images;47 4.1.1;4.1 Introduction;48 4.1.1.1;4.1.1 Problem Statement;50 4.1.1.2;4.1.2 Overview;51 4.1.2;4.2 Technical Description;52 4.1.2.1;4.2.1 Recursive Processing of Data;52 4.1.2.2;4.2.2 The ocfa Library;55 4.1.2.3;4.2.3 The Repository;55 4.1.2.4;4.2.4 Storage of (Dynamic) Metadata;56 4.1.2.5;4.2.5 Interprocess Communication between Modules;56 4.1.2.6;4.2.6 The AnycastRelay and the Router;56 4.1.2.7;4.2.7 The Router Module;58 4.1.2.7.1;4.2.7.1 Rules and the Rulelist;58 4.1.2.8;4.2.8 Available ocfa Modules;59 4.1.2.8.1;4.2.8.1 The Kickstart Module;60

4.1.2.8.2;4.2.8.2 Datastore Module;60 4.1.2.8.3;4.2.8.3 Miscellaneous Modules;61 4.1.2.9;4.2.9 Database Layout and Reporting;61 4.1.2.9.1;4.2.9.1 The Core Tables;62 4.1.2.9.2;4.2.9.2 Additional Metadata Tables;62 4.1.2.9.2.1;Example Generating an Overview of Encountered Mimetypes;62 4.1.2.9.3;4.2.9.3 Searching for Specific Values and Creating Export Shell Commands;63 4.1.3;4.3 User Interface;64 4.1.3.1;4.3.1 Command Line Administration Interface;64 4.1.3.2;4.3.2 Web Interface;65 4.1.3.3;4.3.3 Security;66 4.1.4;4.4 Discussion;66 4.1.4.1;4.4.1 Evaluation;67 4.1.4.2;4.4.2 Future Work;69 4.2;References;69 5;Chapter 5;70 5.1;Open Source Live Distributions for Computer Forensics;70 5.1.1;5.1 Introduction;70 5.1.2;5.2 Related Work;72 5.1.3;5.3 Phases of Digital Investigation;73 5.1.3.1;5.3.1 Information Gathering;73 5.1.3.2;5.3.2 Collection;74 5.1.3.3;5.3.3 Examination and Analysis;74 5.1.4;5.4 CAINE Architecture;75 5.1.4.1;5.4.1 Software Wrapper;75 5.1.4.2;5.4.2 Graphical Interface;76 5.1.5;5.5 Tools Integrated in CAINE;77 5.1.5.1;5.5.1 Information Gathering;77 5.1.5.2;5.5.2 Collection;78 5.1.5.3;5.5.3 Examination and Analysis;78 5.1.6;5.6 Report Building Phase;79 5.1.7;5.7 CAINE Evolution and Validation;80 5.1.7.1;5.7.1 Beta Release;80 5.1.7.2;5.7.2 Early Releases;81 5.1.7.3;5.7.3 Swap Issue and Current Release;82 5.1.8;5.8 Conclusions;82 5.2;References;83 6;Chapter 6;84 6.1;VALI: A Visual Correlation Tool Based on Vector Clocks;84 6.1.1;6.1 In EAN/ISBN : 9781441958037 Publisher(s): Springer, Berlin, Springer US Format: ePub/PDF Author(s): Huebner, Ewa - Zanero, Stefano

[DOWNLOAD HERE](#)

Similar manuals: