

2014

## 12th Australian Digital Forensics Conference, 2014, Edith Cowan University: conference details

Security Research Institute, Edith Cowan University

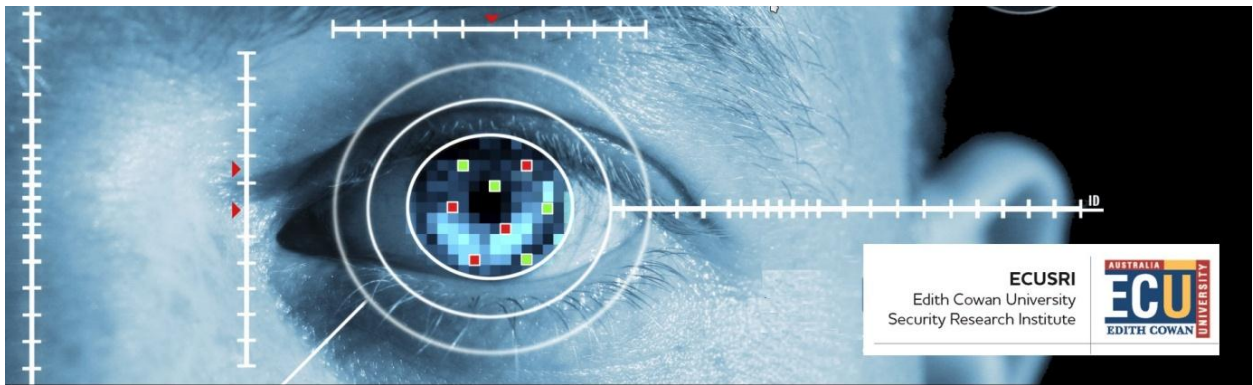
Follow this and additional works at: <https://ro.ecu.edu.au/adf>



Part of the [Information Security Commons](#)

---

This Conference Proceeding is posted at Research Online.  
<https://ro.ecu.edu.au/adf/143>



# The Proceedings of

## 12<sup>th</sup> Australian Digital Forensics Conference

1-3 December, 2014

ECU Joondalup Campus, Perth, Western Australia



Proceedings of the  
12<sup>th</sup> Australian Digital Forensics Conference

**Published By**

Security Research Institute  
Edith Cowan University

**Edited By**

Professor Craig Valli  
Security Research Institute  
Edith Cowan University  
c.valli@ecu.edu.au

Copyright 2014, All Rights Reserved, Edith Cowan University

ISBN 978-0-7298-0719-7

CRICOS Institution Provider Code 00279B

Sponsors

**ECUSRI**  
Edith Cowan University  
Security Research Institute



Supporters



## **Conference Foreword**

This is the third year that the Australian Digital Forensics Conference has been held under the banner of the Security Research Institute, which is in part due to the success of the security conference program at ECU. As with previous years, the conference continues to see a large number of papers with a number of high quality submissions from local and international authors. All submissions were subject to a double blind peer review process and we had an acceptance rate of approximately 80%.

Conferences such as these are simply not possible without willing volunteers who follow through with the commitment they have initially made, and I would like to take this opportunity to thank the conference committee for their tireless efforts in this regard. These efforts have included but not been limited to the reviewing and editing of the conference papers, and helping with the planning, organisation and execution of the conference. Particular thanks go to those international reviewers who took the time to review papers for the conference, irrespective of the fact that they are unable to attend this year.

To our sponsors and supporters also a vote of thanks for both the financial and moral support provided to the conference. Finally, to the student volunteers and staff of the ECU Security Research Institute – your efforts as always are appreciated and invaluable.

Yours sincerely

### **Conference Chair**

Professor Craig Valli, Director, Security Research Institute

### **Congress Organising Committee**

Congress Chair: Professor Craig Valli

Committee Members: Dr David Brooks  
Mr Clinton Carpena  
Mr Jeff Corkill  
Mr Michael Coole  
Mr David Cook  
Mr Michael Crowley  
Mr Peter Hannay  
Dr Mike Johnstone  
Mr Patryk Szewczyk  
Mr Krishnun Sansurooah  
Dr Zubair Baig  
Associate Professor Andrew Woodward  
Associate Professor Trish Williams  
Professor Bill Hutchinson  
Professor Nara Srinivasan

Congress Coordinator: Ms Emma Burke

## Table of Contents

<b>TOWARDS A SET OF METRICS TO GUIDE THE GENERATION OF FAKE COMPUTER FILE SYSTEMS.....</b>	<b>5</b>
<i>Ben Whitham</i>	
<b>LOCATIONAL WIRELESS AND SOCIAL MEDIA-BASED SURVEILLANCE.....</b>	<b>17</b>
<i>Maxim Chernyshev</i>	
<b>THE ZOMBIES STRIKE BACK: TOWARDS CLIENT-SIDE BEEF DETECTION.....</b>	<b>26</b>
<i>Maxim Chernyshev, Peter Hannay</i>	
<b>FORENSIC EXAMINATION AND ANALYSIS OF THE PREFETCH FILES ON THE BANKING TROJAN MALWARE INCIDENTS.....</b>	<b>35</b>
<i>Andri P Heriyanto</i>	
<b>LISTENING TO BOTNET COMMUNICATION CHANNELS TO PROTECT INFORMATION SYSTEMS....</b>	<b>44</b>
<i>Brian Cusack, Sultan Almutairi</i>	
<b>UP-DATING INVESTIGATION MODELS FOR SMART PHONE PROCEDURES.....</b>	<b>53</b>
<i>Brian Cusack, Raymond Lutui</i>	
<b>SUITABILITY OF LACUNARITY MEASURE FOR BLIND STEGANALYSIS.....</b>	<b>64</b>
<i>Ahmed Ibrahim</i>	
<b>A FORENSICALLY-ENABLED IAAS CLOUD COMPUTING ARCHITECTURE.....</b>	<b>75</b>
<i>Saad Alqahtany, Nathan Clarke, Steven Furnell, Christoph Reich</i>	
<b>A USER-ORIENTED NETWORK FORENSIC ANALYSER: THE DESIGN OF A HIGH-LEVEL PROTOCOL ANALYSER.....</b>	<b>84</b>
<i>D. Joy, F. Li, N.L. Clarke, S.M. Furnell</i>	
<b>THE IMPACT OF CUSTOM ROM BACKUPS ON ANDROID EXTERNAL STORAGE ERASURE.....</b>	<b>94</b>
<i>Haydon Hope, Peter Hannay</i>	
<b>A FORENSIC OVERVIEW OF THE LG SMART TV.....</b>	<b>102</b>
<i>Iain Sutherland, Konstantinos Xynos, Huw Read, Andy Jones, Tom Drange</i>	
<b>RAPID FORENSIC CRIME SCENE ANALYSIS USING INEXPENSIVE SENSORS.....</b>	<b>109</b>
<i>Dan Blackman</i>	
<b>FINDING EVIDENCE OF WORDLISTS BEING DEPLOYED AGAINST SSH HONEYPOTS - IMPLICATIONS AND IMPACTS.....</b>	<b>114</b>
<i>Priya Rabadia, Craig Valli</i>	