Project Title

Michael Shell
School of Electrical and
Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
WWW: http://www.michaelshell.org/contact.html

Homer Simpson
Twentieth Century Fox
Springfield, USA
Email: homer@thesimpsons.com

James Kirk
and Montgomery Scott
Starfleet Academy
San Francisco, California 96678-2391
Telephone: (800) 555–1212
Fax: (888) 555–1212

***Abstract*—The abstract goes here.**

***Index Terms*—Computer Society, IEEEtran, journal, LaTeX, paper, template.**

I. Introduction

Give a short description of your study. More importantly, describe the motivation for your study. I wish you the best of success.

II. Background

Use as necessary, adapt to your project, delete or comment out the rest.

Example cites from the outline:

- The primary textbook used for the course is [1].
- There are additional useful resources on the subject that we may refer to for one concept or another throughout the class. They are listed under the “References” section: [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22].

Example cites from the project document:

- ...(e.g., set up a CVS [23], SVN [24], Git [25], etc. repository) to share...
- ...Or easychair [26], single column, LaTeX.... ...For a succinct introduction to LaTeX please see [27] as well as [28]....
- ...For projects that involve Forensic Lucid [18], contact the instructor for more details. See the corresponding examples of encoding data in Forensic Lucid format in [18, Chapter 9] in meantime....
- ...Provide thorough formalization (of known evidence and hypotheses) of informal case studies in our textbook [1, Chapters 3, 7], and other sources covered in class, such as [29] in Forensic Lucid...
- ...Hands-on use of Sleuthkit [8], Autopsy [30], and other tools in a simulated investigation, reasoning, analysis, and reporting. It is not guaranteed it will be possible to use the commercial tools like FTK [31] or EnCase [32], [33]....
- ...The sample data would come from the honeynet [34] and DFRWS [35] projects/challenges:...
- ...Revival of the Ftklipse [20], [21], [22] project with MARFCAT and MARFPCAT plug-ins, and possibly distributed system evaluation integration....
- ...Implementation and possibly verification of Forensic Lucid encoders [19] for different popular server software as plug-ins or modules to provide functionality to the said servers to log their data directly in Forensic Lucid and/or write translation tools (scripts) to translate existing logs into Forensic Lucid, e.g., any two from Apache, Tomcat, Dovecot, Syslog, BIND [36], `iptables` [37], [38], `sshd`, JSON data, or others of your choice. Discuss with the instructor....
- ...The encoder verification sub-project may involve Isabelle/HOL [39], [40] to show that any log or data structure translation done is faithful enough and no meaning loss or corruption occurs....
- ...Formalize Forensic Lucid in Z [41], [42] and verify the past sample Forensic Lucid investigative specifications using Z tools....

A. Sub-section 1

Discuss papers related to your study. Break into sub-sections if necessary [43], [44], [45].

B. Sub-section 2

1) Subsubsection Heading Here: Subsubsection text here. Cite per IEEE guidelines [46].

C. Summary

Synthesis and summary of findings from the rest of the background, etc.

III. Metrics

A. Metrics definition

Provide a formal definition for the metrics used in your study. Use a separate sub-section for each metric. You may add small computation examples for the metrics you consider more difficult to understand. The rest will go into the background.

B. Metrics calculation/implementation details

Provide interesting implementation details for the more challenging metrics you implemented as well as tools used.

IV. Empirical Study

Provide a high-level description of the study Use subsections as necessary per project specification. Below are some examples.

A. *Examined variables*

Describe your independent and dependent variables.

B. *Examined hypotheses*

Describe the null and alternative hypotheses.

C. *Experiment design*

List the projects you have selected for the analysis. Justify your selection. Describe their characteristics (size, history, version, revisions, development team, development practices, etc.)

D. *Data collection*

Describe the way that you collected the data (developed techniques for data collection, used tools, etc.)

E. *Statistical analysis*

Statistical tests. Discussion of the results.

F. *Threats to validity*

Internal, External, Construct validity.

TABLE I
AN EXAMPLE OF A TABLE

One	Two
Three	Four

V. CONCLUSION

The conclusion goes here.

ACKNOWLEDGMENT

The authors would like to thank...

REFERENCES

[1] P. Boismenu, *INSE691E: Cybercrime Investigation, Lecture Notes*. Concordia University, 2012.

[2] S. Anson, S. Bunting, R. Johnson, and S. Pearson, *Mastering Windows Network Forensics and Investigation*, 2nd ed. Sybex, Jun. 2012.

[3] C. Thuen, "Understanding counter-forensics to ensure a successful investigation," [online], University of Idaho, 2007, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.138.2196.

[4] C. D. Ball, "Helping lawyers master technology," [online], blog, column, publications, 2006–2013, http://www.craigball.com/Ball_Technology.

[5] The Honeynet Project, *Know Your Enemy*, 2nd ed. Honeynet, 2004.

[6] K. Mandia, C. Prosise, and M. Pepe, *Incident Response and Computer Forensics*, 2nd ed. McGraw-Hill, 2003.

[7] C. Pearce, "Helix: Open-source forensic toolkit," [online], Apr. 2005, http://www.e-fense.com/helix.

[8] B. D. Carrier, "The Sleuth Kit," [online], 2006–2015, http://www.sleuthkit.org/sleuthkit/.

[9] D. Mares, "Software links for forensics investigative tasks," [online], 2006, http://www.dmares.com/maresware/SITES/tasks.htm.

[10] A. R. Arasteh and M. Debbabi, "Forensic memory analysis: From stack and code to execution history," *Digital Investigation Journal*, vol. 4, no. 1, pp. 114–125, Sep. 2007.

[11] A. R. Arasteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," *Digital Investigation Journal*, vol. 4, no. 1, pp. 82–91, Sep. 2007.

[12] R. Hadjidj, M. Debbabi, H. Lounis, F. Iqbal, A. Szporer, and D. Benredjem, "Towards an integrated e-mail forensic analysis framework," *Digital Investigation*, vol. 5, no. 3-4, pp. 124–137, 2009.

[13] P. Gladyshev, "Formalising event reconstruction in digital investigations," Ph.D. dissertation, Department of Computer Science, University College Dublin, Aug. 2004, online at http://www.formalforensics.org/publications/thesis/index.html.

[14] P. Gladyshev and A. Patel, "Finite state machine approach to digital event reconstruction," *Digital Investigation Journal*, vol. 2, no. 1, 2004.

[15] P. Gladyshev, "Finite state machine analysis of a blackmail investigation," *International Journal of Digital Evidence*, vol. 4, no. 1, 2005.

[16] M. Debbabi, "INSE 6150: Lecture 6: Formal analysis (II)," Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada, 2006, http://www.ciise.concordia.ca/~debbabi.

[17] ——, "INSE 6120: Cryptographic protocols and network security, lecture notes," Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada, 2005, http://users.encs.concordia.ca/~debbabi/inse6120.html.

[18] S. A. Mokhov, "Intensional cyberforensics," Ph.D. dissertation, Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Sep. 2013, online at http://arxiv.org/abs/1312.0466.

[19] S. A. Mokhov, M. J. Assels, J. Paquet, and M. Debbabi, "Automating MAC spoofer evidence gathering and encoding for investigations," in *Proceedings of The 7th International Symposium on Foundations & Practice of Security (FPS'14)*, ser. LNCS 8930, F. Cuppens *et al.*, Eds. Springer, Nov. 2014, pp. 168–183, full paper.

[20] M.-A. Laverdière, S. A. Mokhov, D. Bendredjem, and S. Tsapa, "Ftklipse – Forensic Toolkits Eclipse Plug-ins," SourceForge.net, 2005–2008, http://ciisesec.svn.sourceforge.net/viewvc/ciisesec/forensics, last viewed April 2008.

[21] M.-A. Laverdière, S. A. Mokhov, S. Tsapa, and D. Benredjem, "Ftklipse–design and implementation of an extendable computer forensics environment: Software requirements specification document," 2005–2009, http://arxiv.org/abs/0906.2446.

[22] ——, "Ftklipse–design and implementation of an extendable computer forensics environment: Specification design document," 2005–2009, http://arxiv.org/abs/0906.2447.

[23] D. Grune, B. Berliner, D. D. Z. Zuhn, J. Polk, L. Jones, D. R. Price, M. D. Baushke, B. Murphy, C. T. Pino, F. U. M. ao, J. Hyslop, and J. Meyering, "Concurrent Versions System (CVS)," [online], 1989–2014, http://savannah.nongnu.org/projects/cvs/.

[24] CollabNet, Inc., "Subversion (SVN)," [online], 2006–2014, http://subversion.tigris.org/.

[25] S. Potter, "Git," in *AOSA, Volume II*, 2012, http://aosabook.org/en/git.html.

[26] S. A. Mokhov, G. Sutcliffe, and A. Voronkov, "The easychair class file documentation and guide, for authors and editors," [online], 2008–2011, available at http://easychair.org/easychair.zip.

[27] P. Grogono, *A LaTeX2e Gallimaufry. Techniques, Tips, and Traps*. Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Mar. 2001, http://www.cse.concordia.ca/~grogono/Writings/gallimaufry.pdf, last viewed May 2014.

[28] Wikibooks, "LaTeX — Wikibooks, The Free Textbook Project," [Online; accessed 14-May-2014], 2014, http://en.wikibooks.org/w/index.php?title=LaTeX&oldid=2632161.

[29] A. Bennett and M. J. Assels, "Computer security at Concordia: Past problems, proposed plans," [online], 1995–1998, http://spectrum.library.concordia.ca/980620/.

[30] B. D. Carrier, "Autopsy forensic browser," [online], 2006–2013, http://www.sleuthkit.org/autopsy/.

[31] AccessData, "FTK – Forensic Toolkit," [online], 2008–2013, http://www.accessdata.com/products/digital-forensics/ftk.

[32] Guidance Software, "EnCase," [online], 1997–2015, http://www.encase.com/.

[33] S. Bunting, *EnCase Computer Forensics – The Official EnCE: EnCase Certified Examiner Study Guide*, 3rd ed. Sybex, Sep. 2012.

[34] Honeynet Project, "Honeynet forensics project scans," [online], 2002–2015, http://old.honeynet.org/scans.

[35] G. Palmer (Editor), "A road map for digital forensic research, report from first digital forensic research workshop (DFRWS)," DFRWS, Tech. Rep., 2001.

[36] P. Albitz and C. Liu, *DNS and BIND*, 3rd ed. O'Reilly, 1998, ISBN: 1-56592-512-2.

[37] G. N. Purdy, *Linux iptables: Pocket Reference*. O'Reilly, 2004, ISBN: 978-0-596-00569-6.

[38] M. Rash, *Linux Firwalls: Attack Detection and Response with iptables, psad, and fwsnort*, 3rd ed. San Francisco: No Starch Press, Inc., 2007, ISBN: 978-1-59327-141-1.

[39] L. C. Paulson, T. Nipkow, and M. Wenzel, “Isabelle: A generic proof assistant,” [online], University of Cambridge and Technical University of Munich, 2007–2015, http://isabelle.in.tum.de/, last viewed October 2015.

[40] T. Nipkow, L. C. Paulson, and M. Wenzel, *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. Springer-Verlag, Nov. 2007, vol. 2283, http://www.in.tum.de/∼nipkow/LNCS2283/, last viewed: December 2007.

[41] A. Velykis, L. Freitas, M. Utting, P. Dietrich, and T. Miller, “The Community Z Tools (CZT) project,” [online], 2003–2015, http://czt.sourceforge.net.

[42] J. M. Spivey, *The Z Notation: A Reference Manual*, 2nd ed. Prentice Hall, 1992, http://spivey.oriel.ox.ac.uk/mike/zrm/index.html.

[43] M. Lanza and R. Marinescu, *Object-Oriented Metrics in Practice: Using Software Metrics to Characterize, Evaluate, and Improve the Design of Object-Oriented Systems*. Springer, 2006.

[44] S. A. Mokhov, J. Paquet, and M. Debbabi, “The use of NLP techniques in static code analysis to detect weaknesses and vulnerabilities,” in *Proceedings of Canadian Conference on AI’14*, ser. LNAI, M. Sokolova and P. van Beek, Eds., vol. 8436. Springer, May 2014, pp. 326–332, short paper.

[45] R. Marinescu, “Measurement and quality in object-oriented design,” Ph.D. dissertation, Politehnica University of Timisoara, Romania, 2002.

[46] L. Hughen and IEEE, “IEEE citation reference,” [online], 2007–2009, http://www.ieee.org/documents/ieeecitationref.pdf.