UNIVERSITY OF OXFORD
SOFTWARE ENGINEERING PROGRAMME

Wolfson Building, Parks Road, Oxford OX1 3QD, UK
Tel +44(0)1865 283525 Fax +44(0)1865 283531
info@softeng.ox.ac.uk www.softeng.ox.ac.uk

Part-time postgraduate study in software engineering

Forensics, FOR

14th – 18th October 2013
ASSIGNMENT

The purpose of this assignment is to test the extent to which you have achieved the learning objectives of the course. As such, your answer must be substantially your own original work. Where material has been quoted, reproduced, or co-authored, you should take care to identify the extent of that material, and the source or co-author.

Your answers to the questions on this assignment should be submitted to:

Software Engineering Programme
Department of Computer Science
Wolfson Building
Parks Road
Oxford OX1 3QD

Alternatively, you may submit using the Software Engineering Programme website — `www.softeng.ox.ac.uk` — following the submission guidelines. The deadline for submission is 12 noon on Tuesday, 3rd December 2013. If you have not already returned a signed assignment acceptance form, you must do so before the deadline, or your work may not be considered. We hope to have results and comments available during the week commencing Monday, 13th January 2014.

ANY QUERIES OR REQUESTS FOR CLARIFICATION REGARDING THIS ASSIGNMENT SHOULD, IN THE FIRST INSTANCE, BE DIRECTED TO THE PROGRAMME OFFICE WITHIN THE NEXT TWO WEEKS.

---

1 Introduction

This assignment concerns the analysis of evidence from a Linux laptop computer.

The assignment allows you to demonstrate your understanding of the tools that are used to analyse computing device evidence, and that you understand how to conduct a forensic investigation involving computing device evidence.

2 Requirements

Assignment: Part 1

Computer intrusion for espionage or malicious intent is well documented. Computer intrusions using networks have occurred to such a degree that analysis has revealed that the tactics and procedures taken by the intruders tend to follow a similar pattern.

The intruder is likely to go through a number of steps prior to a network-based intrusion and after the intrusion. The steps could be broadly characterised as:

- Planning
- Mobilization
- Action [The network-based intrusion which itself is broken into a number of phases.]
- Assessment

Question1: Describe a typical network-based intrusion scenario and the phases involved in attacking the target. Focus your description on the activities of the intruder and explain what the intruder expects to achieve in each phase.

Question 2: Describe the potential evidence that you maybe able to recover and analyse from the computer used by the intruder to perform these steps. Consider what evidence maybe recoverable from the computer system and applications used for communications (such as email), intrusion (such as nmap and Metasploit.)

Assume that the intruder has used a typical computer system and has not used a live distribution nor have they encrypted data so that you cannot recover it.

Do not focus on the potential evidence that would be left on the system being intruded.

Assignment: Part 2

Perform a forensic analysis of the laptop computer evidence on the accompanying DVD. Document your approach and findings in a manner suitable for use in a legal case. Produce an investigation report along with any additional documentation such as an investigation protocol, your notes, chain of custody forms, etc., as you feel is appropriate.

Background to the investigation:

On or about August 21st Mr. Samuel Pepys created a server to allow him to publish a blog and to exchange emails with friends and colleagues. Mr. Pepys works for the King Charles' government in the Royal Navy Office in London. This is a time of heightened tension as the Anglo-Dutch War continues. On August 25th Mr. Pepys noticed that his blog had been defaced.

At the end of August 2012, Alexandrine de Rye, Countess of Thurn and Taxis, was stopped on the Belgium border attempting to cross into The Netherlands. As she was suspected of owing VAT the police held her for questioning and retained a laptop computer in her possession. However due to the Europe-wide issues associated with mislabeled meat, an administrative error led to Countess de Rye being released while her laptop was retained but not analysed. The laptop has now made it into the possession of King Charles' spymaster.

An image has been made of the sda1 hard disk partition on Alexandrine de Rye's laptop.

You have been assigned to work on this case by King Charles' prosecutor. The prosecutor needs your opinions on the following questions:

1. What had Countess de Rye used the laptop for and how was it setup? Whom, if anyone, had Alexandrine de Rye communicated with using the laptop?
2. Did Countess de Rye attack Mr. Pepys' server and if so how?

   If Countess de Rye did attack Mr. Pepys' server:
3. Was Alexandrine de Rye working for and/or with anyone else?
4. Did Alexandrine de Rye deface the blog and if so how?
5. Was information on the server viewed or taken (in addition to any viewing of the blog)? Identify the information that has been (or may have been) taken or viewed.
6. Was any information passed to a 3rd party?
7. If possible identify the location that the attack originated from?

Your opinions on these questions should be given in the Investigation Report.

Provided Materials

1) DVD1 with the raw image from laptop hard disk partition sda1 imaged on June 30th, 2013;
2) "DVD Investigator" holds a virtual machine for the student to use to undertake the forensic analysis. This is the same virtual machine that was used in the class exercises. Username: forensic. Password: oucl2013.
3) The ssh_host_rsa_key.pub for pepys.dyndns.org is:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAwvjhTkleDoJCOQYt5
FMw1ngiirVX/A/nG331P8oX6skXqM/F+wIFKQvlUX0qwcl5EC
80t/2VXNKBkjAIinH3lEhjLif4VgAmbRNdLm4dHNaOcg/MP5i
MjDbh8TY7T9bzMMRv1G/dAMJii+yxKcxGSdBQJeryCYi1UCT
PIqtWpZckHxqTJ8keyyPuF5sYDvjAPAehfOBai1WkQdejPv6jWf
5b1ZuifMzFSuvzxy5zRSABiP9FSBTz78ImCBaGQE91lH8THd6
8/bxmVzcJEJDzHz1Zt4d/hSy/b+X6k+g9QUOvYz9rafFoTkAu3X
7T1GnMO9a2i4k4hR1I/wj6WQHuoQ== root@pepys.dyndns.org
```

Deliverables

A written response for Part 1. An Investigation Report and associated documentation for Part 2.

Page Limits

Part One:

Maximum 10 pages if including drawings, typically 5 pages.

Part Two:

Maximum of 40 pages for all material submitted;

Investigation Report, typically 10 – 20 pages;

Protocol, typically 2 – 5 pages;

Evidence Log, typically 2 pages;

Notes and any other material, typically up to remaining page count.

Pasting evidence into your written assignment response may result in your documentation exceeding the page limit. If there is a large piece of evidence that you think is significant and you want to refer to it in your report, précis your findings and include the evidence as an electronic-only item with your submission. Label the file as **<your name> electronic-only**. That way it will not be printed out but still be made available to the examiners. Simply sending back all your evidence will not result in marks being given. The evidence returned must be relevant to what is discussed in your assignment.

3 Guidance

Please structure your answer so that there is a cover sheet, which contains *only* your name, the subject and date, and a note of the total number of pages. Do not put any answer material on the cover sheet; begin your answer on a fresh page. Avoid putting your name on any page except the cover page. Please, do number the pages and sections.

Evidence should support your opinions.

In addition to your investigation report you should also provide documentation on how you conducted your investigation and analysis. This additional documentation could represent:

1) The protocol that you followed;
2) Notes and records you made in the course of your investigation;
3) Additional, associated and relevant evidence uncovered during the course of the investigation.

The investigation report is expected to be a type written document, in hard copy. The investigation report shall have a minimum font size of 12pt except for tables

and graphics, which shall have a minimum font size of 10pt. The additional documentation can be in the form of legibly hand written notes, typed records, labelled/identifiable computer print-outs, labelled / identifiable / referenced electronic files.

The investigation report would be expected to have a structure similar to this:

Introduction
Background
Sequence of Events and Description of Incident
Evidence and Analysis
Findings/Opinions
Conclusions

However you may add or subtract from this as you feel is appropriate.

[Editorial

The assignment implies the evidence has been created using real computers. In fact some evidence may have been created using virtual machines. For the purposes of this assignment treat the evidence as if it has come from real hardware. If you find any artifacts associated with virtual machines treat them as you would a real artifact. There is no need to ponder a conspiracy with the evidence gathering.]

Dr. Gareth Digby

July 13th, 2013

4 Assessment criteria

The aim of the assessment is to discover the extent to which the student has achieved the learning outcomes of the course:

1) The student has understood the principles of computer forensic investigation and analysis;
2) The student has understood and practiced using the processes and procedures taught in the module;
3) The student has understood and practiced using the tools and techniques described in the module;
4) The student is able to suitably evaluate computer system(s) in an unfamiliar scenario and discuss their findings in a suitable manner.

Appropriate application of the principles taught in the course will offer an excellent means of demonstrating the relevant capabilities.

5 Attributions

Material used in creating the evidence for this assignment is derived from *The Diary Of Samuel Pepys* website, http://www.pepysdiary.com, run by Phil Gyford.

The copyright for *The Diary Of Samuel Pepys* website, http://www.pepysdiary.com, is as follows:

- The main diary entries, their footnotes, the text in the Diary Introduction section, and the text from 1893 in some Encyclopedia topics are taken from the Project Gutenberg version of Pepys' diary and as such are free of copyright restrictions.
- All annotations added by users in the Diary section, Encyclopedia and the rest of the site are available under a Creative Commons Attribution-NonCommercial-ShareAlike license unless specified otherwise. Any material posted in the annotations by users that is quoted from elsewhere retains its original copyright status.