

# SANCHIT KARVE

<http://www.sanchitkarve.com> ▪ [✉ write2sanchit@gmail.com](mailto:write2sanchit@gmail.com) ▪ [\(425\) 985-6945](tel:(425)985-6945) ▪ Portland, Oregon

## Objective

To obtain a full-time position that enables me to use my skill sets in software development, reverse engineering or application/network security.

## Highlights

- Extensive experience in application development (client and server side), Mobile Applications development and Reverse Engineering.
- Moderator on large online programming forums (like dreamincode.net, with more than 500,000 members) with a passion for teaching and helping co-developers solve problems.
- Ardent programmer proficient in a variety of software tools and technologies and having expertise in C/C++, Python, x86 assembly.
- One of the few researchers in the security industry with knowledge of the esoteric Visual Basic 6 file format and its runtime internals.

## Skill Set

Programming Languages	Advanced : C, Python, x86 Assembly Moderate : C++, C#, PHP, JavaScript, Java SE/ME/Android
Databases	Advanced: MySQL Moderate: MongoDB, Amazon S3, SQL Server
Operating Systems	Advanced: Windows Moderate: Linux (Debian-based distros) Familiar: Mac OSX
Reverse Engineering/Security Tools	Advanced: IDA Pro, OllyDbg, HIEW, WireShark Moderate: WinDbg

## Education

Masters in Computer Science (M.S.) - HCI major	Oregon State University	Sep 2010 – Sep 2012
Bachelor of Engineering (B.E.) - Computer Engineering	University of Mumbai, India	Jun 2006 – Jun 2010

## Work Experience

### Anti-Malware Researcher – McAfee Inc.

Sep 2012 – present

I research malware and their infection vectors for Windows and Linux and develop internal tools for malware unpacking and analysis, automation, clustering, threat intelligence and signature development. I author and improve detection and repair code for McAfee's VirusScan line of products as a result of analyzing various parasitics, trojans, anti-emulation techniques and advanced persistent threats. My research on the Sality file infector has enabled McAfee to be the only anti-malware product to completely restore infected samples down to the last byte. Recently I authored an automation system to mimic network communication (with custom encrypted protocols) of three malware families with their control servers and harvested ~25,000 unique samples over a period of around 6 months. Awarded McAfee Labs' Employee of the Quarter for Q1 2013 and Collaboration Award for Q3 2013.

Posts on McAfee Labs Blog: <http://blogs.mcafee.com/author/sanchit-karve>

### Maintainer – The Privly Foundation

Oct 2011 – present

Volunteering with an open source project called Privly as their maintainer of their Opera browser extension and Android app. Mentored a student to develop the android app during Google's Summer of Code (GSoC) 2013 and GSoC 2014.

Project URL: <https://www.priv.ly>

### Graduate Research Assistant – Oregon State University

Sep 2010 – Sep 2012

Researched Reusability of Software Components on Online Repositories by analyzing "low ceremony evidence" such as reviews/comments, age, usage statistics, etc. of source code posted on CodeProject.com and SourceForge.net to predict its quality.

Thesis: <http://ir.library.oregonstate.edu/xmlui/handle/1957/33638>

Publication: <http://dl.acm.org/citation.cfm?id=2465459>

### Software Engineering Intern – Electro-Scientific Industries (ESI), Portland, OR

Jun 2011 – Sep 2011

Worked on the GUI (C#) and Control Programs (C++) of ESI's 3500 (Multi-Layer Ceramic Capacitor Tester) and 3800 (LED Tester) models.

- 1) Added Multi-threading functionality in the 3500 to speed up the process of finding the ideal vibration frequency of its feeder.
- 2) Created a Custom Version Controller for Visual Studio 2008/2010 that incorporates Changeset IDs from Team Foundation Server (TFS), Build Accounts, TFS Branch Labels, etc. into the Application's manifest.
- 3) Added software licensing code to provide access to 3500's Stress Test features only to licensed users.
- 4) Created a Diagnostic Tool capable of creating and editing Simulation Test files for the 3800 LED Tester.
- 5) Added graphing functionality in the 3500 GUI to present a visual representation of data from log files.
- 6) Added code to reduce number of sensors required to detect bin drawer states in the 3500.
- 7) Extended existing code to support an additional shim sensor in the 3500.

3500 Project URL: <http://www.esi.com/Products/PassiveComponents/ElectricalTesters.aspx>

3800 Project URL: <http://www.esi.com/Products/PassiveComponents/LEDTesters.aspx>

**Student Developer – Oregon State University (Business Solutions Group – Software Dev.)**

Feb 2011 – Jun 2011

1) Helped develop a system called Transportation Operating Center System (TOCS) using C# for the Oregon Department of Transportation (ODOT) to consolidate data for 4 regional dispatch centers throughout the state and integrating multiple software systems.

Project URL: <http://bsg.oregonstate.edu>

**AI Developer – Oregon State University (School of Electrical Engineering and Computer Science)** Oct 2010 – Jan 2011

Ported and tested an MS-Outlook plugin written for Outlook 2007 to work with Outlook 2010. Used VSTO with C# for creating an interface between the Outlook plugin, a SOAP/WSDL web service and Java sockets. Also wrote and tested code for generating and reading data formatted in XML and JSON using C#. "TaskTracer" is a Task-Based Interruption Recovery & Knowledge Management tool to investigate the possibilities of a desktop software system that will track in detail how knowledge workers complete tasks and intelligently leverage that information to increase efficiency and productivity.

Project URL: [http://web.archive.org/web/20120419111316/http://tasktracer.osuosl.org/?page\\_id=181](http://web.archive.org/web/20120419111316/http://tasktracer.osuosl.org/?page_id=181)

**Notable Projects:****Thallium Backup**

Using: Java (Android), BusyBox, PHP, Amazon S3

Wrote an open source alternative to Titanium Backup to allow users with rooted phones to backup and restore their apps and data. Integrated with Amazon S3 to enable cloud backups.

Project URL: <https://github.com/born2c0de/ThalliumBackup-Android>

**Privly**

Using: JavaScript, Java (Android)

Helped write and maintain the browser extensions for Opera and Chrome for an open source project called Privly. Mentored a student to develop the android app during GSoC 2013. Presented project at Open Source Bridge conference in Portland, Oregon in June 2012.

Project URL: <https://github.com/privly>

Conference Session: <http://opensourcebridge.org/sessions/788>

**Incrementor for Sublime Text 3**

Using: Python

Ported and extended the Incrementor Plugin to Sublime Text 3. Accepted into the Package Control manager.

Project URL: <https://github.com/born2c0de/Incrementor/>

**Facebook/Twitter Redirect Fixers for Chrome and Opera**

Using: JavaScript

A browser extension focused on privacy to prevent facebook and twitter from learning which links you click while browsing their websites. This is implemented by modifying the DOM to remove any redirection from external URLs.

Project URL: <http://sanchitkarve.com/projects/facebookredirectfixer/>

**SourceForge.net Project Review Summarizer**

Using: NLP, C#, SourceForge.net Read-Only API

Used a set of NLP techniques to retrieve the quality of features of open-source software from their reviews on SourceForge.net

**Universal Mobile Device Synchronization**

Using: PHP, J2ME, C#

This system enables users to synchronize their personal information seamlessly across mobile devices and computers irrespective of the device platform. UMDS was written at a time when no solution existed to wirelessly synchronize information across devices.

Project URL: <http://www.sanchitkarve.com/umds>

**PocketFare – Mumbai**

Using: J2ME, PHP, Java for Android

This system enables users to view the latest fares for the taxis and auto-rickshaws of Mumbai, India. A daily newspaper "Maharashtra Times", which has a readership of over 1 million, published an article about this application in August 2010. Also appeared for a live television interview on a national news channel TV9 (Hindi) about the app.

Project URL: <http://www.sanchitkarve.com/projects/pocketfaremumbai>

**BunkM – Mobile Attendance Manager**

Using: J2ME, PHP

This project enables students from Indian Universities to manage their attendance and check if they need to attend additional lectures to fulfil the minimum attendance requirement for their course. It also features a backup system where users can upload and download their attendance information on the web server. A daily newspaper "Maharashtra Times", which has a readership of over 1 million, published an article about this application in September 2010.

Project URL: <http://www.sanchitkarve.com/projects/bunkm>