DFIR Prague 2014
Summit Agenda

SUNDAY 5 OCTOBER - MORNING

8:00 - 9:00 am	**Registration & Coffee**
9:00 - 09:15 am	**Welcome** Jess Garcia, SANS Institute
9:15 - 10:00 am	**Rekall - We can remember it for you wholesale!** Rekall is a new memory analysis framework. Originally forked from the Volatility code base, Rekall is a complete memory analysis and acquisition solution. It includes acquisition software for OSX, Linux and Windows with many advanced features not found in other acquisition solutions. Rekall features an interactive user interface which can be used for creating reports of the analysis work. Additionally, Rekall can be used as a library as part of a larger system, with a flexible data export layer. This talk will examine some of the new features introduced to the Rekall framework, and how it can be used to analyse memory. We also examine how Rekall can be used as part of a large distributed forensic application, namely the GRR project. Michael Cohen, Google
10:00 - 10:20 am - - - **NETWORKING BREAK** - - - 10:00 - 10:20 am	
10:20 - 11:15 am	**The Social Media Connection & Potentially Unwanted Advice** The latest threats have one thing in common: in one way or another they are using Social Media. Social Media is of course fun, a way to stay in contact with your friends and a way to "share" your activity. But it also carries unexpected dangers. These include not only accidental but unwanted exposure (specifically, pictures), but also exposure to malicious URLs and cybercriminal activities like click-jacking. With a little social engineering you click the links and are taken for a bumper car ride down the cybercrime highway - once something is on the internet, one way or the other, it is always available, even if you think it has been removed. The presentation explores various aspects of Social Media, the different dangers from both the social and cybercriminal point of view, and the potentially irreversible and damaging consequences of unexpected exposure. Each example will be illustrated with real-life stories, some with less than desirable consequences, to say the least. One real-life story will be fully examined showing what can happen when social media meets cybercrime - what you can lose, what it will cost. Although not all problems can be solved by security solutions, examples and suggestions are given to better protect the end-user, both at home as well as at the corporate end-point. Those who think that the corporate end-points are not at risk are ill advised. Righard Zwienenberg, ESET
11:15 am - 12:00pm	**Finding the needle in the haystack with ELK** Incident handlers and forensic analysts are all confronted with the same problem: Finding a needle in a haystack, without knowing what the needle looks like. It doesn't really matter if this haystack is made out of proxy logs, email logs, timelines, dns logs, ids, ... But what matters are the techniques we use to look at this data and find quickly what we are looking for. In this presentation we will tackle these problems with a combination of three tools: Elasticsearch, Logstash and Kibana. This trio known as ELK has grown immensely in popularity since the creation of the company in 2012. It is attracting users from the leaders like Splunk, ArcSight, ELSA and co. Together they provide a very powerful blazing-fast open source data analytics tool. Real-time or completely offline. In a single node, in a cluster or in a distributed architecture. This presentation is highly recommended if you want to work faster with and get more out of things like: mactime, proxy logs, supertimeline, plaso, mail logs, (passive) dns logs, firewall logs, syslog, ... Christophe Vandeplas, Belgian Federal Government
12:00 - 1:15 pm - - - **LUNCH** - - - 12:00 - 1:15 pm	

SUNDAY 5 OCTOBER - AFTERNOON

1:15 - 2:00 pm

Give me the password and I'll rule the world

There is a gold mine of information indirectly protected by the Windows user's credentials: Encrypted File System files, picture password, fingerprint password, WiFi passwords, RSA private keys and so on. DPAPI (Data Protection API) is the Windows component in charge of encrypting and decrypting them given the user's password. Moreover, many applications rely on DPAPI services to protect their data: so, even if many clear text artifacts are available, knowing the encrypted information will help push-on the investigation.

The password is the lever and DPAPI is the place to stand, but what if the password is unknown? Apart from cracking attempts, do we have something else we can use? And then how to get the desired info using DPAPI?

The presentation will introduce the DPAPI component, then it will describe how and when it is possible to get the user password without cracking. It will cover the opportunity to unlock DPAPI even without the cleartext password and, finally, a couple of third-party applications will be examined to show the benefits of this offensive digital investigation approach.

Francesco Picasso, REALITY NET System Solutions

2:00 - 2:45 pm

Collaborative timeline analysis in large incidents

Have you ever felt that your current tools are limiting your ability to share your findings effectively within your team? And that they undermine you when collaborating with your fellow responders?

Or that you cannot reuse knowledge obtained from previous incidents?

In this presentation we take a look at how you can utilize Open Source digital forensic software to overcome some of these obstacles. We discuss several tools that make up a powerful toolbox that allows you to focus on the incident related knowledge, questions and answers and not the nitty gritty detail of the tools. We show you how to handle large scale incidents with a new powerful way of analyzing timelines.

Johann Berggren, Google

2:45 - 3:15 pm --- NETWORKING BREAK --- 2:45 - 3:15 pm

3:15 - 4:00 pm

Windows ShellBags Forensics In-Depth

The problem of identifying when and which folders a user accessed arises often in digital forensics. Forensicators attempt to search for them in the ShellBags information because it may contain registry keys that indicate which folders the user accessed in the past. Their timestamps may demonstrate when the user accessed them. Nevertheless, a lot of activities can update the timestamps. Moreover, the ShellBags structure differs slightly between different Windows operating systems. How to interpret ShellBags correctly has become a challenge. This presentation summarizes the details of ShellBags information and discusses various activities across Windows operating systems.

Vincent Lo, Klein & Co. Computer Forensics

4:00 - 4:45 pm

Forensic Analysis of MySQL-Database Systems

This presentation will demonstrate a simple approach to forensic analyses of MySQL-Database systems which are based on Debian operating systems. Furthermore this presentation will show the different artefacts on the operating system and database system levels (especially Storage Engine InnoDB), which are relevant for forensic research. This process will only use open source tools. To improve the forensic process, the speaker developed two python scripts to automate steps within this forensic analysis. This scripts are not finished for production use yet, so attendees could get involved in this project. The scripts are not finished for production use yet, so attendees could get involved in this project. The attendees should have a basic understanding of Linux, MySQL-DBMS and the hexadecimal number system.

Marcel Niefindt, proXcel GmbH

4:45 - 5:15 pm

The Fast Four Finale

Four quick and intense presentations covering an area of importance and relevance to the presenter in a compressed format. These skills changed the outcome of a case on which they were working!

Pasquale Stirparo - mac4n6 artifacts library - One location to rule them all

Mattia Epifani - Tor Forensics on Windows

Righard Zwienenberg - PUA/PWS Potentially Unwanted Advise/Potentially Wanted Solution

Vincent Lo - ShellBag Analysis Tools

5:15 - 6:00 pm

Q&A

Jess Garcia chairs an open forum in which attendees can ask questions of today's presenters.