<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 - 9:00 am</td>
<td>Registration &amp; Coffee</td>
</tr>
<tr>
<td>9:00 - 9:15 am</td>
<td>Welcome</td>
</tr>
<tr>
<td>Jess Garcia, SANS Institute</td>
<td></td>
</tr>
<tr>
<td>9:15 - 10:00 am</td>
<td>Rekall - We can remember it for you wholesale!</td>
</tr>
<tr>
<td>Michael Cohen, Google</td>
<td></td>
</tr>
<tr>
<td>10:00 - 10:20 am</td>
<td>Networking Break</td>
</tr>
<tr>
<td>10:20 - 11:15 am</td>
<td>The Social Media Connection &amp; Potentially Unwanted Advice</td>
</tr>
<tr>
<td>Righard Zwienenberg, ESET</td>
<td></td>
</tr>
<tr>
<td>11:15 am - 12:00 pm</td>
<td>Finding the needle in the haystack with ELK</td>
</tr>
<tr>
<td>Christophe Vandeplas, Belgian Federal Government</td>
<td></td>
</tr>
<tr>
<td>12:00 - 1:15 pm</td>
<td>Lunch</td>
</tr>
</tbody>
</table>
## 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**

### 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. Forensic examiners 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
Richard 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.