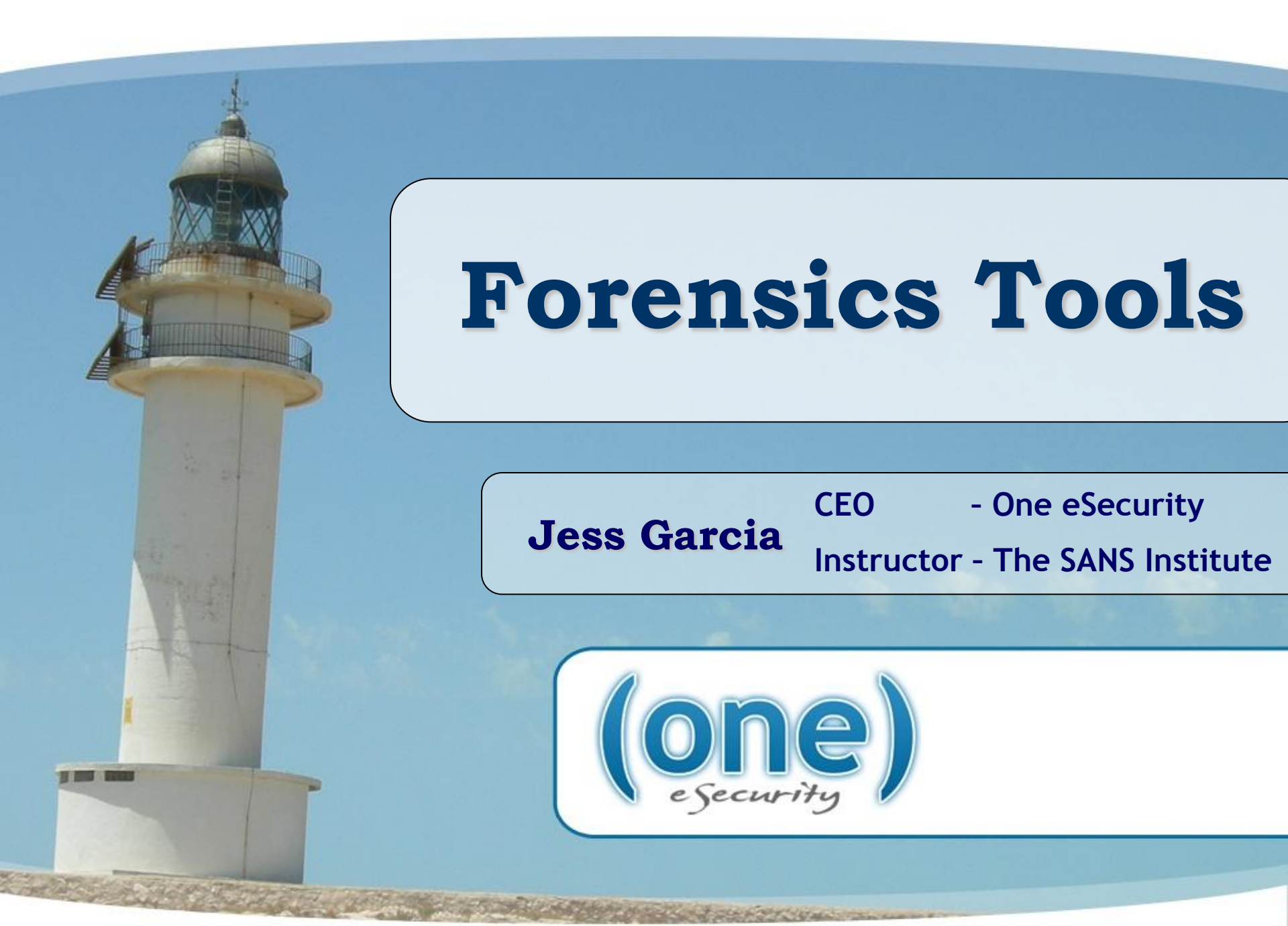


Forensics Tools

Jess Garcia

CEO - One eSecurity

Instructor - The SANS Institute

(one) eSecurity

Jess Garcia

- SANS Instructor
  - Forensics & Malware Analysis
- Founder of One eSecurity
- 15+ Years in Computer Security
  - 10+ Years in Computer Forensics
- 10 years at the Spanish DoD
- 5 years as a Private Sector Consultant
  - Customers Worldwide: Financial, Government, Law Firms, Corporate, …

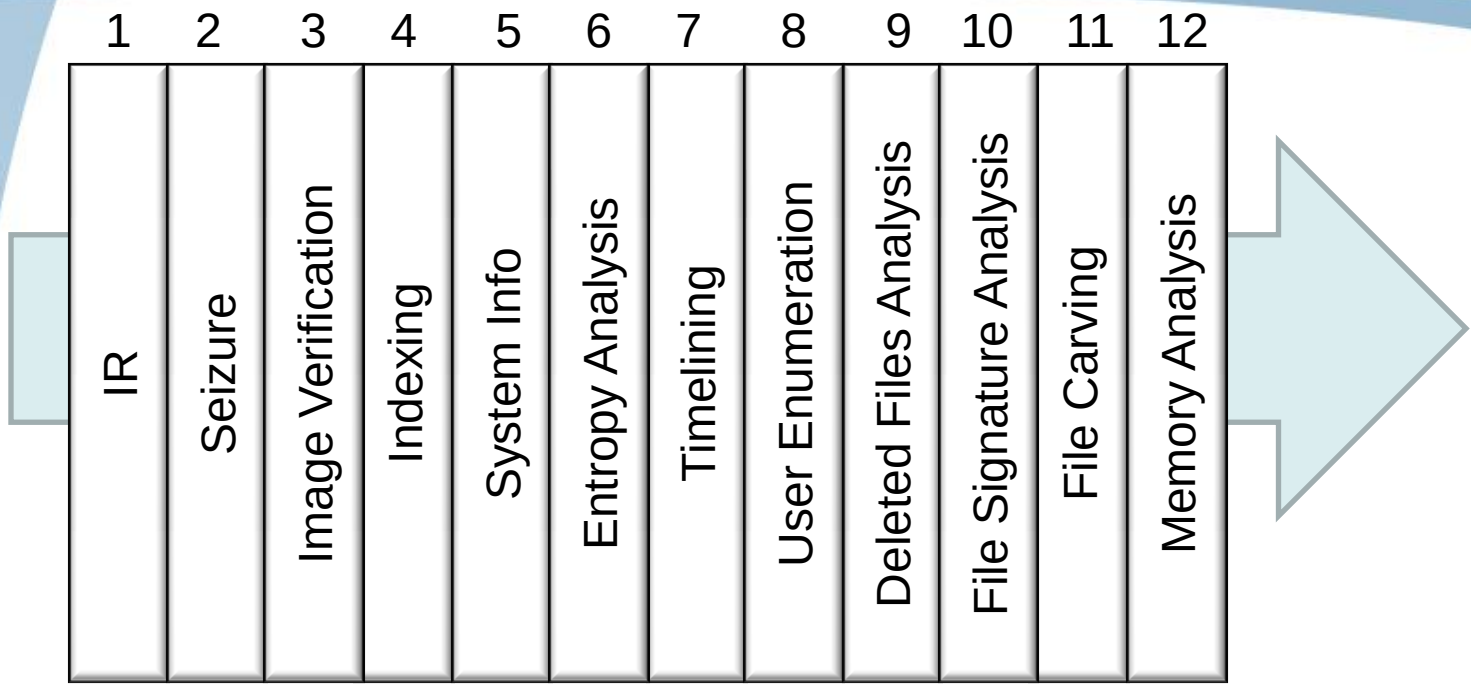
Question

What software do you routinely use working with cases?

Why was it useful and is this capability found in other competing software products?

The Forensics Process

Mainstream Analysis



1. Helix, EnCase-E, WFT, …
2. Helix, FTK Imager, EnCase-E
3. *sum, Suites
4. FTK
5. EnCase
6. FTK, ent
7. Mactime
8. EnCase, FTK
9. Sleuthkit
10. sorter, Suites
11. Foremost, scalpel
12. Volatilty

The Forensics Process

Specific Analysis

User Analysis	Data Recovery
Email Analysis	Partition Recovery
Browser Analysis	Metadata Recovery
Activity Analysis	Media Recovery

OTHER

Log Analysis	Filesystem Analysis	Artifact Analysis
Traffic Analysis	Malware Analysis	Password Recovery

Automation, Correlation & Advanced Analsysis

- Non-Forensics Tools
  - Native Platforms
- Scripts & Programs
  - bash, perl, C, EnScript, python, …
- FOREST
  - FOrensics REsponse SysTem
  - Automated Analysis Framework
  - Integrates with the previous tools
  - Correlates Tools & Sources

3 Real World Examples

- Spionage Case
  - SSL Interception (ssldump)
  - Web Proxy
- Fraud Case
  - Heavily Overwritten Outlook File
  - Advanced Filesystem Recovery
  - Tested 15+ Outlook Tools
- Massive Seizure & Analysis
  - DoJ Investigation
  - 150+ computers / 10+ countries

YOU ARE THE MOST POWERFUL TOOL!

Challenges

- Standardization
- Certification
- Automation
- Storage Size
- Forensics “on the Cloud”
- Forensics can be everything

About One eSecurity

Download the latest version at:

www.one-esecurity.com/SANSIR09.pdf

www.one-esecurity.com

USA: +1 202 470 0730

UK: +44 208 123 5211

Email me at:

jess@one-esecurity.com