RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: **MASH-T10**

Explore Adventures in the Underland: Forensic Techniques against Hackers Evading the Hook

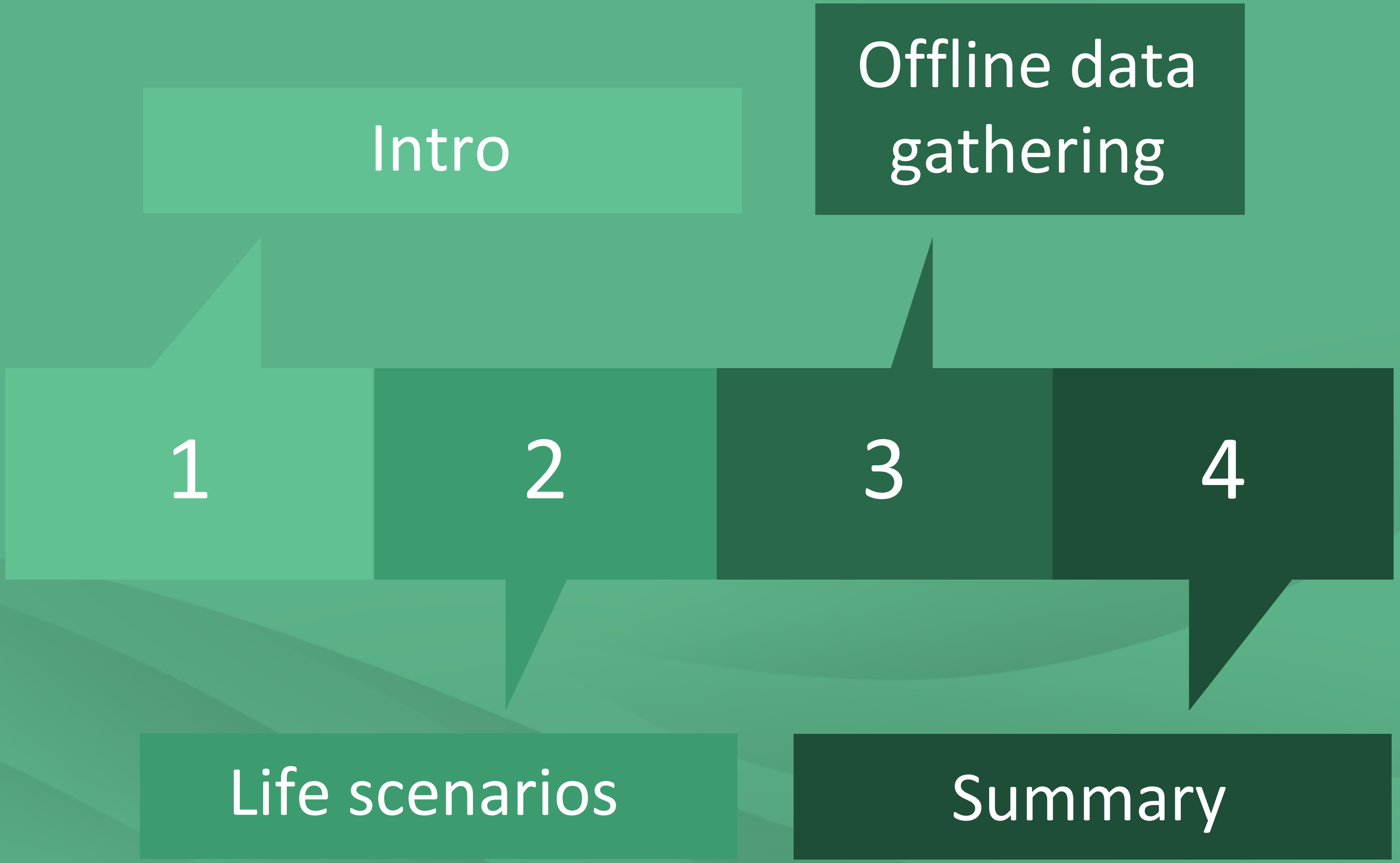
Paula Januszkiewicz

CEO CQURE, Cybersecurity Expert
cqure.pl, cqureacademy.com
paula@cqure.us
@PaulaCqure

Mike Jankowski - Lorek

CQURE, Database and Machine Learning Expert
cqure.pl, cqureacademy.com
mike@cqure.pl
@MJL_PL

Agenda



1 Intro

2 Life scenarios

3 Offline data gathering

4 Summary

There is pretty much always something you can find…

Searching for a Trace: Memory

Memory

- Handles
- Processes
- Hidden Processes (ActiveProcessLinks)
- Files that can be extracted
- Threads
- Modules
- Registry
- API Hooks
- Services
- UserAssist
- Shellbags
- ShimCache
- Event Logs
- Timeline

Searching for a Trace: Disk

Disk

- Profile, NTUSER
- Run dialog
- Most Recently Used (MRU), Management Console (MMC)
- Remote Desktop connections
- Prefetch files
- Recent documents
- Automatic Destinations (LNK)
- Security Log
- RDP Operational Log
- Application Logs
- Temporary Internet Files
- Deleted files – recoverable from the disk
- NTFS Structures
- Hiberfil.sys
- Memory dumps

Techniques for Hiding vs. Recovering Data

File Level Games

- Extension change
- Joining files
- Alternative data streams
- Embedding
- Playing with the content
- Steganography
- Deletion

Disk Level Games

- Hiding data
- Encryption

Forensics adventures: Summary

- Make sure all tracing features on the drive and in the system are enabled: USN, Prefech etc.
- Image first then play
- Create Incident Response Procedure (most of the Customers we start the adventure with do not have it…)

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Password: CQUREAcademy#123!

What does CQURE do?

1. Consulting Services:

- Extensive IT Security Audits and Penetration Tests of all kinds,
- Configuration Audit and Architecture,
- Design Social Engineering Tests,
- Advanced Troubleshooting and Debugging,
- Emergency Response Services.

2. R&D & CQLabs Tools & Hacks Publications

3. Trainings & Seminars:

- Offline (mainly in New York or via our partners worldwide),
- Online.

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **MASH-T10**

Explore Adventures in the Underland: Forensic Techniques against Hackers Evading the Hook

Paula Januszkiewicz

CEO CQURE, Cybersecurity Expert
cqure.pl, cqureacademy.com
paula@cqure.us
@PaulaCqure

Mike Jankowski - Lorek

CQURE, Database and Machine Learning Expert
cqure.pl, cqureacademy.com
mike@cqure.pl
@MJL_PL

#RSAC