Cybersecurity Forensics Workshop

Incident Analysis, Cyber Forensics,
and Engagement with Law Enforcement

Michael Lewis,
Deputy Director, Q-CERT

Clear Your Mind …

… then, think of your favorite old detective show …

… And, quick, picture the crime scene!


E SCENE
OT CROSS

The Classical TV Crime Scene

- Yellow tape surrounding the scene
- White chalk outlining the body (there's almost always a body)
- A forensics guy, whose name you usually didn't know, dusting for fingerprints
- And the star: a middle-aged, slightly overweight, rumpled detective, who spends most of his time social-engineering the suspects!

A TV “CSI” Crime Scene

- The entire program is built around the forensics guys … and ladies!
- And much of the time is spent in the laboratory, scientifically analyzing evidence such as hair samples, paint chips, and dirty shoes

A Modern Crime Scene

- A growing percentage of actual crimes do not involve bodies, or getaway cars, or guns, or even an explicit crime scene
- Rather, they utilize computers, and networks
- And much of the evidence is hidden amongst thousands of files and transactions, on dozens of different digital devices

The Investigation

- The classical forensics techniques used by investigators must be updated to include the identification, retention, and analysis of digital devices
- Traditional techniques may inadvertently damage digital evidence, or render it unusable in court

A Walk-through

The agenda includes a review of a crime scene, and the description and demonstration of several key investigative and forensic techniques

The Agenda

1. Presentation of an Incident
2. Forensically-Safe Investigative Techniques
3. Live Memory Acquisition and Analysis
4. Device Imaging and Analysis
5. The Role of Expert Witnesses
6. Engagement with Law Enforcement
7. Reviewing the “Results” of our Investigation
8. Final Comments

Incident Background

- 1 January 2008 – The annual financial report for Khalid's Acme Widgets Limited Company is pre-released to Board members.
- 2 February - Hamid's Widgets Inc. makes a hostile bid to take over Khalid Acme's Widgets Limited Company.

Coincidence?

- The hostile bid incorporates “insider” information
- The Board believes that confidential information was leaked.
- The Chief Information Officer is asked by the Board to conduct an internal investigation

Initial Investigation

The CIO requests a review of internal data from the preceding 3 months.

The HR director reports a coincidence: the Office Administrator gave unexpected 30-day notice of resignation on 2 January, and left on 1 February.

A Security Officer discovers security video of suspicious activity in a particular office.

Surveillance video shows shredding of documents after hours!

Unauthorized use of an office machine!

The Request for Assistance

- The CIO gathers the information and reports to the Board.
- The Board believes that the events may be related and could be criminal, and contacts law enforcement.
- In the course of the investigation, law enforcement contacts the national information security team for technical assistance.

The Scene of the Crime

The Suspects

The IT department has identified five individuals who had access to the office and its computers

- The sales director
- The receptionist
- The technical assistant
- The office manager
- And an unexpected outsider

Raj Neely

Sales Director

Born in Namibia to Moravian missionary parents, lived in Qatar in 70’s, family banned, returned in ’98.
Launched Qatar United Application Consultant King (QUACK)

Renny “Red” O’Donnell

Receptionist

English citizen, Army veteran, former game show host in Britain, previously employed by Al Jazeera, owner of local shawarma stand.

Robert “Robbie” Williams

Technical Assistant

Irish national, born in Cambodia, resident of Doha for six years, long history of making “suggestions” to management to improve operations.

Natasha Gameova

Office manager

Age: depends on how she feels

Russian born, circus-trained.

Speaks Russian, English, French, Armenian, Afghani and Arabic

Raquel Maroni

Daughter of the network administrator.

When questioned, she claimed she was trying to load her favorite video game!

Digital Devices of Interest

- Desktop computer
- Laptop computer
- External hard drive
- USB drive
- Personal Digital Assistant (PDA)
- Digital Camera
- MP3 Player

Examples from our Scene

Digital devices require special care and processing

1. Identify the items
2. “image” the items
3. Store the originals
4. Analyze the images

A Quandary

How can we distinguish innocent or slightly mischievous behavior from genuinely criminal conduct?

What if the investigation uncovers activities outside the scope of the original investigation?

As we shall see …

- Examine the scene
- Conduct a “forensically safe” investigation
- Capture any “live” sessions
- Image and analyze all digital devices
- Assess the results – what is known? With what level of assurance?

Thanks!

To the members of the Doha Players for their time and creativity in assisting our presentations:

Kerry Suek as Raj Neely

Dima Issa as Natasha Gameova

Ian Mckay as “Robbie” Williams

Sabrina Young as “Red” O’Donnell

Rachel Marella as Raquel Maroni