eForensics

eForensics

Discovery and analysis of evidence of Computer Crimes

- Crimes against computers
- Involving computers
- Or, where computers contain evidence of non-computer-rated crimes

Types of eForensics

Network forensics

- Packet capture, logs – record evidence while the crime is occurring.
- Cloud forensics – relies on cooperation of cloud provider, cloud API, foreign government.

Disk forensics/phone forensics

- Live (no re-boot)
- Dead/offline/static (boot into another OS)
- Acquisition (of drive image)
- Acquisition (of RAM)

Types of Forensics

Memory forensics

- Contents of RAM,
- running processes,
- active network connections (TCP) and
- Traffic (UDP)

Disk Forensics

- **Different sorts of evidence available depending on platform, OS, file system.**
- **Want to get meta-data as well as files.**
- **Meta-data provides nexus information:**

– Who, what, when, where.

– Proof that the suspect did the crime.

– Who’s account did they use?

First steps

- **Secure crime scene, confiscate computer.**
- **Record all running processes,**
- **Record system time (compared to actual time)**
- **Record partition details, drive mapping**
- **If drive cannot be imaged, plug in a write-blocker**

– Prevents metadata from being changed

Use toolkits

Linux Distros.

- Caine
- Backtrack
- Knoppix
- Helix
- SANS SIFT

FTK (Forensic ToolKit)

TSK (The Sleuth Kit)

Autopsy (front end for TSK)

EnCase (Windows)

Steps

1. Make a forensic copy of drive.
2. Calculate a hash of the copy for later.
3. Record the time on the computer, compare with actual.
4. Impound drive as evidence.
5. Note down everything that follows so that another forensic expert can find the same evidence.

Analysis of Image

1. **Load into tool, check hash.**
2. **Search for deleted files.**
3. **Search for re-named files (esp. file extensions).**
4. **Search for encrypted containers.**
   - Use entropy analysis to determine type of encryption.
   - Search drive for password reminders…
5. **Search for keywords in files.**
6. **Search for e-mails, shortcuts, file shares, favourites, cached web files.**

File Carving

1. **Search for keywords in deleted file space (even if it’s reformatted, repartitioned).**
2. **Find sectors containing keywords**
3. **Find iNodes containing sectors**

– Or find starting signature, end signature sectors.

4. **Copy sector range to file**
5. **View**

Found evidence?

1. When files “of interest” are found, record metadata, copy of file, file location.
2. Dates are very important – establish a time-line which reflects the sequence of events during the crime.
3. If Wireshark captures or logs are found, use these to confirm times, sequence of events.
4. Check hash again.
5. Write report.