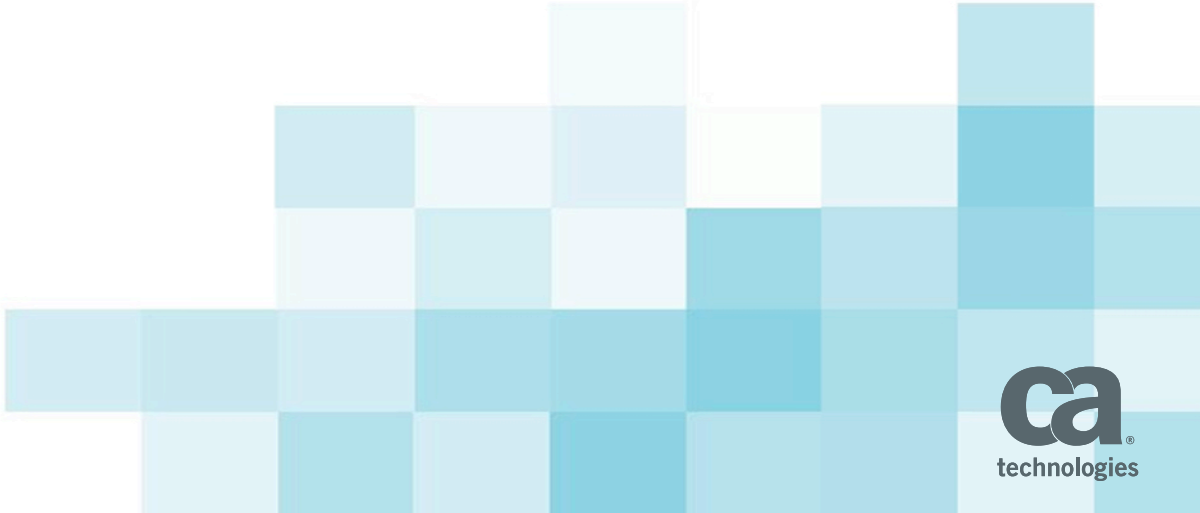
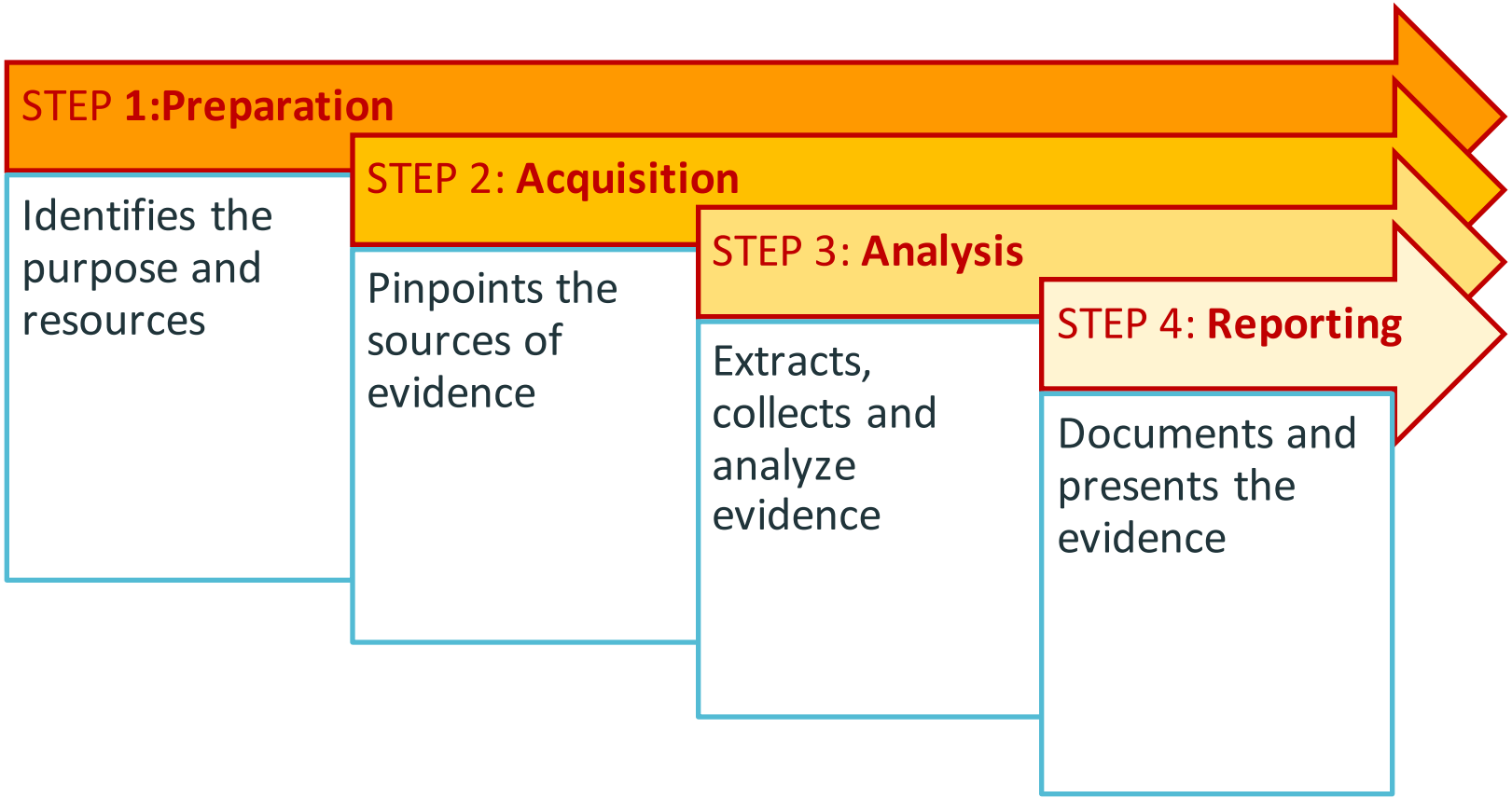
Cybersecurity Forensics

Dipto Chakravarty
SVP, Core Security
July 26, 2016



ca technologies

Forensics 101

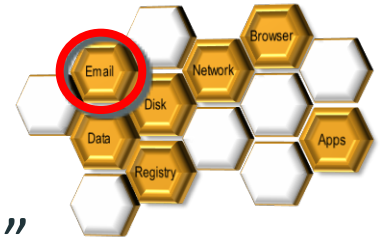


2

Types of Cyber Forensics

3

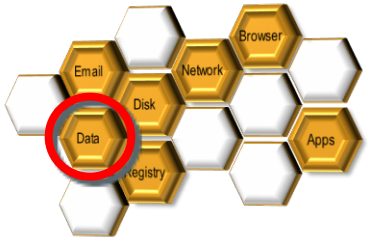
Cyber Forensics: Emails



- "Emails are like footprints in the snow."
- Deleting an email doesn't mean it erases the records. The work is similar to conventional detective work.
- MiTec Viewer
  - Reads Outlook Express, Windows Live Mail with search and filtering capabilities
- PST-OST Viewer
  - Allows you to view Outlook files without MS Exchange

4

Cyber Forensics: Data



- Data mirroring is key in cyber forensics. Exact copy is created without alteration.
- Live View
  - Creates a VM of a physical disk. Allows us to view the data blocks with a user persona and full UX.
- DumpIt
  - Creates executable on USB for rapid IR needs.

5

Cyber Forensics: Disk

- Disk imaging in cyber forensics involves recovery of hidden and erased files. Exact copy is created without alteration.
- Recuva
  - Free tool. Recovers deleted files from disks as well as SD cards, flash drives and cameras
- EDD
  - For rapid IR, it is used as an encrypted disk detector. It checks for encrypted volumes, and tells which transient evidences need to be saved.

6

Cyber Forensics: Registry

- ‘R’ Forensics is about extracting *contextual metadata* more than the data or the user.
- MuiCache
  - Views the list in the MuiCache. (It is the Registry key that stores list of every application installed on the Windows o.s)
- USBDview
  - Lists all USBs connected to the computer (now or earlier!)
  - For each USB, it cites dev type, S No, vendor id, date, etc.

7

Cyber Forensics: Network

- 'N' Forensics is about monitoring traffic, i.e, "data in motion" with the intent to collect evidence/samples.
- Wireshark
  - Popular tool, with both hackers and law enforcements.
  - Inspects frames → captures packets → displays user-data in its own GUI for analysis
- Network Miner
  - Windows-specific tool to detect open ports of network hosts.
  - Popular tool for network forensics analysis.

8

Cyber Forensics: Browser

- ‘B’ Forensics is all about scanning the session trail left behind in the browser cache. Note that almost every browser uses a cache to expedite internet surfing.
- MyLastSearch
  - Scans the cache and browser history files looking for searches you’ve made with popular search engines and social networking sites.
- ChromeCacheView
  - Reads the cache folder to display cached files, URLs, access time, file type, etc. Similar tools exist for other browsers.

9

Cyber Forensics: Apps

- ‘A’ Forensics comprises of reading the app-specific log files without knowing the application password.
- SkypeLogView
  - Displays details of incoming/outgoing calls, chat messages, and file transfers made by the Skype account.
- Y! Messenger Decoder
  - Views the chat sessions, sms, private messages, including emoticons without knowing the password. Similar tools exist for other browsers.

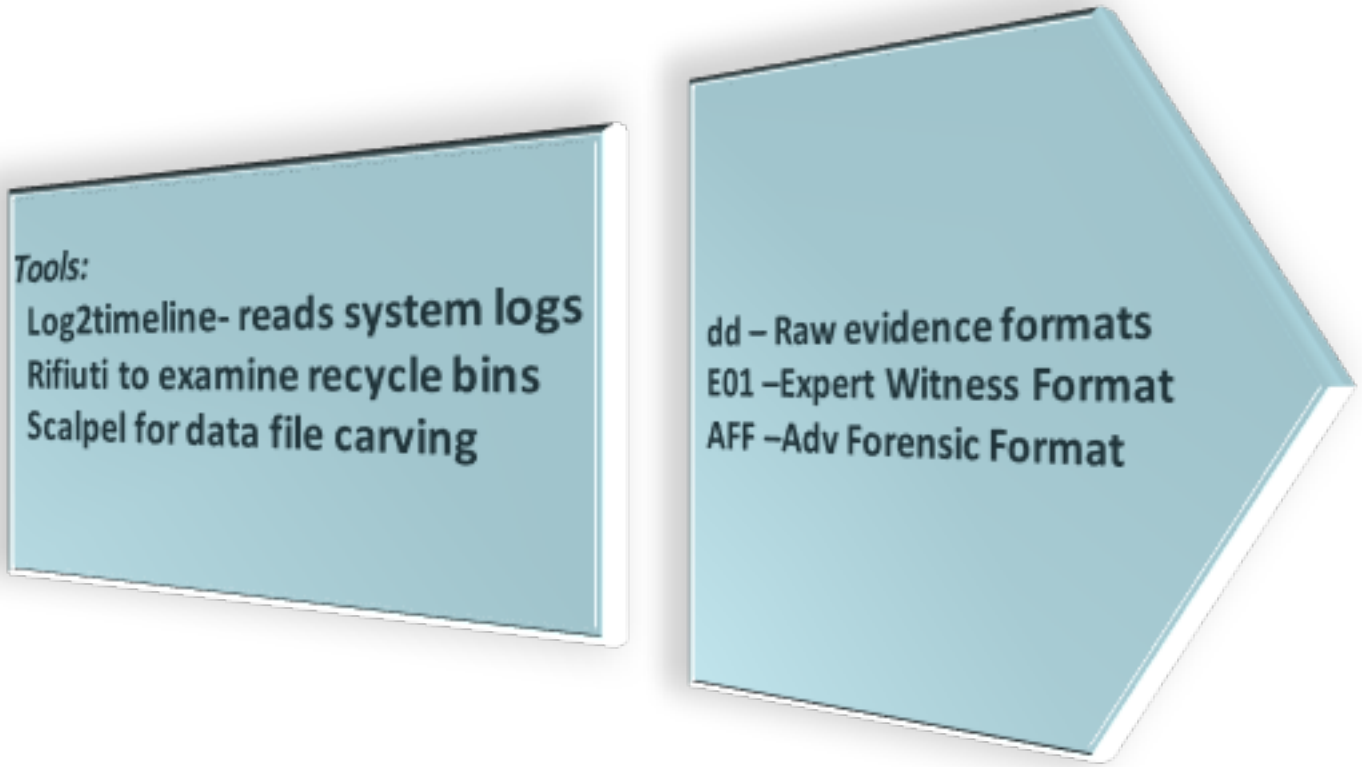
10

General Tools for Forensics Investigation

1. SANS SIFT
2. Linux ‘dd’
3. Xplico
4. The Sleuth Kit
5. Hex Editor Neo
6. Oxygen Forensic Suite http://www.nist.gov/itl/ssd/cs/forensics-tool-testing.cfm

11

SANS Sift – Investigative Forensic Toolkit



12

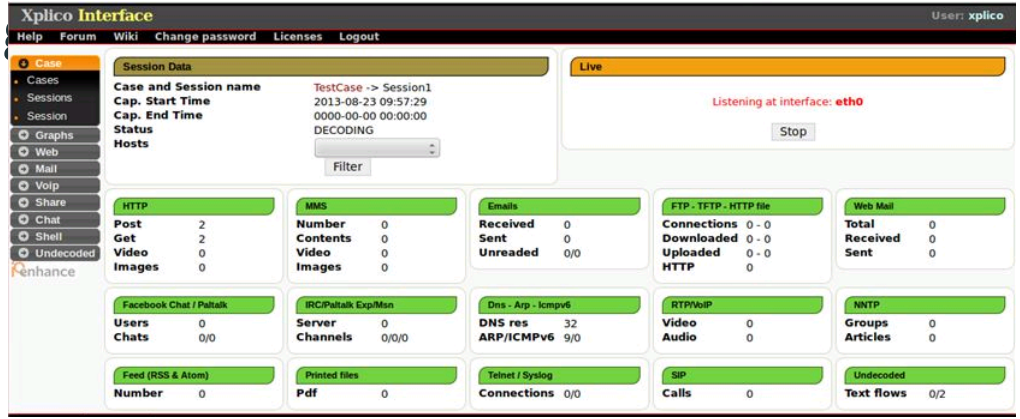
Linux ‘dd’ – Investigative Uses

- Available on almost all Linux o.s distributions
- Used for multifarious forensic tasks, including
  - Forensically wiping a drive
    - **`dd if=/dev/zero of=/dev/drv1 bs=1024`**
    - where if = input file, of = output file, bs = byte size
  - Creating raw image of a drive
    - **`dd if=/dev/drv1 of=/home/diptoc/newimage.dd bs=512 conv=noerror,sync`**
    - where bs = byte size, conv = conversion option
- Very powerful tool. Handle with care.
- *Old is gold!* In use ‘dd’ since 1984

13

Xplico – Investigative Uses

- Open source tool for network forensic analysis
- Extracts application data from the net traffic, e.g.



14

Synopsis of Cyber Forensics Tools & Techniques

- Iterative process
- Best of breed tools
- 360 coverage
- Step by step: prepare, acquire, analyze, report

15

Summarizing Cyber Forensics Principles

- **Assess** user activity w.r.t usage patterns
- **Analyze** data remnants in transient states
- **Audit** logs to unravel stealth data that's encrypted
- **Assert** usage of content and contextual artifacts
- **Answer** the hard stuff:

16

Thank You!

Dipto Chakravarty
On LIn, Tw: @dipto
dipto.chakravrty@ca.com

© Scott Adams, Inc./Dist. by UFS, Inc.