Forensic Investigation

Ben Hung

December 28, 2002

安全焦点
www.Xfocus.org

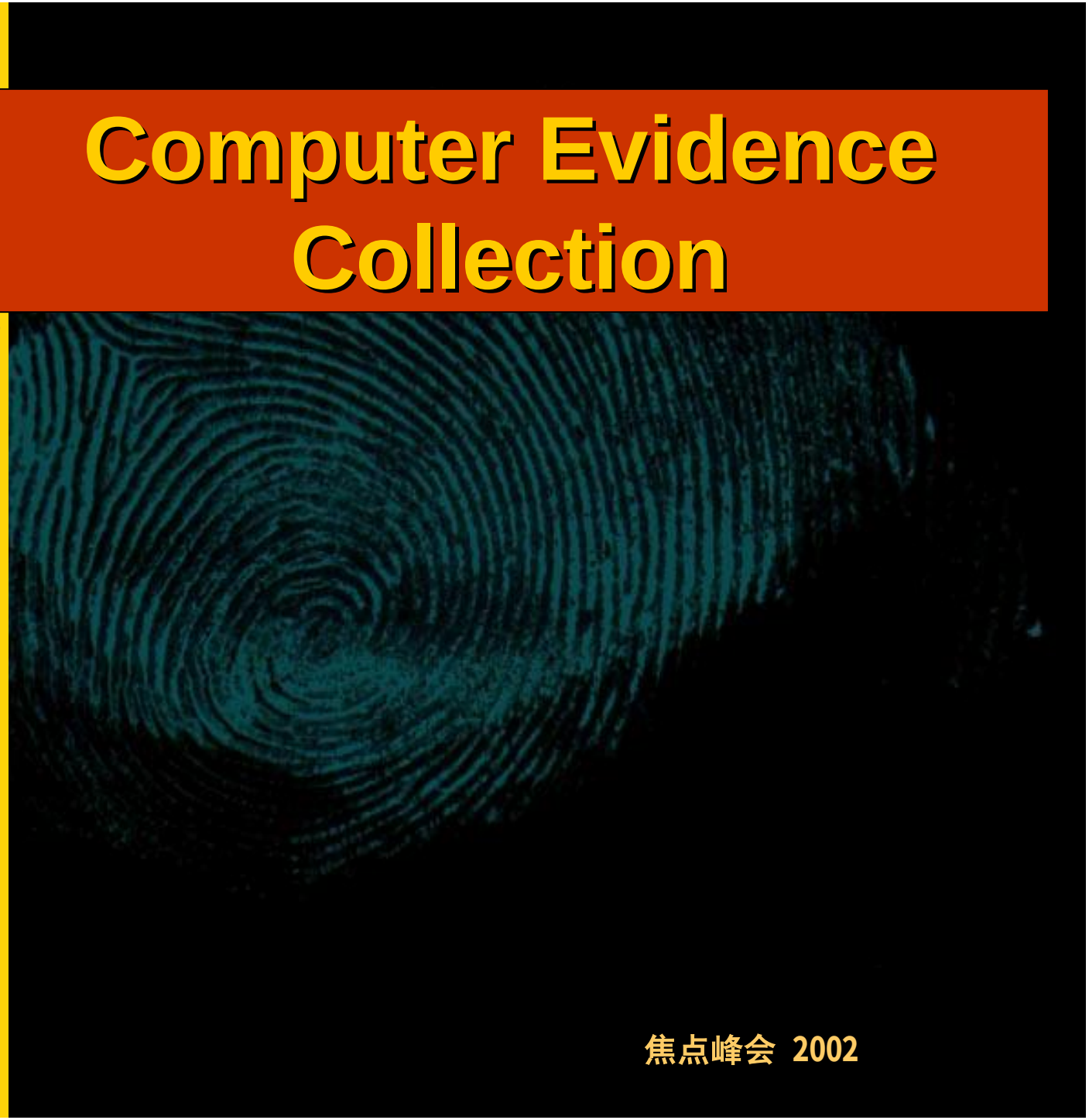
焦点峰会 2002

Agenda

- Computer Evidence Collection using Forensic Tools
- People Evidence Collection through Forensic Interview
- Case Study

安全焦点
www.Xfocus.org

Computer Evidence Collection



安全焦点

www.Xfocus.org

焦点峰会 2002

Computer Evidence Collection

3 Phases Approach

- Phase 1: Preparation
- Phase 2: Data Collection
- Phase 3: Data Analysis

安全焦点
www.Xfocus.org

Preparation Phase

- Step 1: Observe, assess, then move when enemy away
- Dynamic vs Static Data
- Step 2: Static Data:
  - Clone system disk thru 'dd'
  - mount the clone disk on a standalone clean system, as data disk for analysis
- Step 3: Dynamic Data:
  - Do it On Compromised host
  - Disconnected from network first
  - prepare your own system binary on CDROM or diskette

Data Collection Phase

- **Tools**
  - Coroner's Toolkit
    - Grave robber
    - Mactime
    - Unrm
    - Lazarus
  - Mac robber (similar to grave-robber with –m option)
  - Md5, lsof
  - chkrootkit

Data Collection Phase

- **Run "grave-robber –v $mntpoint" on clone disk to collect initial data**
  - Will run set of tools under $TCT/lib.
- **Run MacRobber or "grave-robber –m" to collect MAC attribute**
  - Mac-robber $dir > output.mac
  - Mactime –b output.mac > output.txt
- **Browsing thru the clone disk to collect additional data**
- **Collected data stored on the new system. (do not saved on the clone disk)**

Data Collection Phase

- **Output of "grave-robber –v" put under $TCT/data/$host/ with following directories:**
  - command_out
  - strings_log
  - body
  - body.S
  - coroner.log
  - error.log
  - deleted_files
  - pcat
  - conf_vault

Data Collection Phase

- **Example output of mactime:**
  - Dec 16 01 10:29:06 1585 m.. -rwxr-xr-x root/smtp root tmp/.new/sz
  - Dec 16 01 10:29:11 1595 m.. -rwxr-xr-x root/smtp root tmp/.new/szl
  - Dec 16 01 10:29:41 4692 m.. -rwxr-xr-x root/smtp root tmp/.new/cleaner
  - Dec 18 01 10:01:30 226 m.. -r--r--r-- root/smtp other tmp/.new/default
  - Dec 18 01 18:15:32 670 m.. -rwxr-xr-x root/smtp root tmp/.new/basepatch
  - Dec 27 01 14:00:59 118319 m.. -rw-r--r-- nobody nobody tmp/checkout
  - Jan 03 02 09:34:04 471 m.. -rwxr-xr-x root/smtp root tmp/.new/patch.sol5
  - Jan 04 02 16:36:56 41 m.. -rw-r--r-- nobody nobody tmp/search
  - Jan 31 02 21:51:57 276480 m.. -rw-r--r-- ronnie 100 tmp/eggdrop/scripts/netbots4.05.tar
  - Feb 09 02 12:05:52 620 m.. -rwxr-xr-x root/smtp root tmp/.new/patch.sol6
  - Feb 09 02 13:14:30 683 m.. -rwxr-xr-x root/smtp root tmp/.new/procs

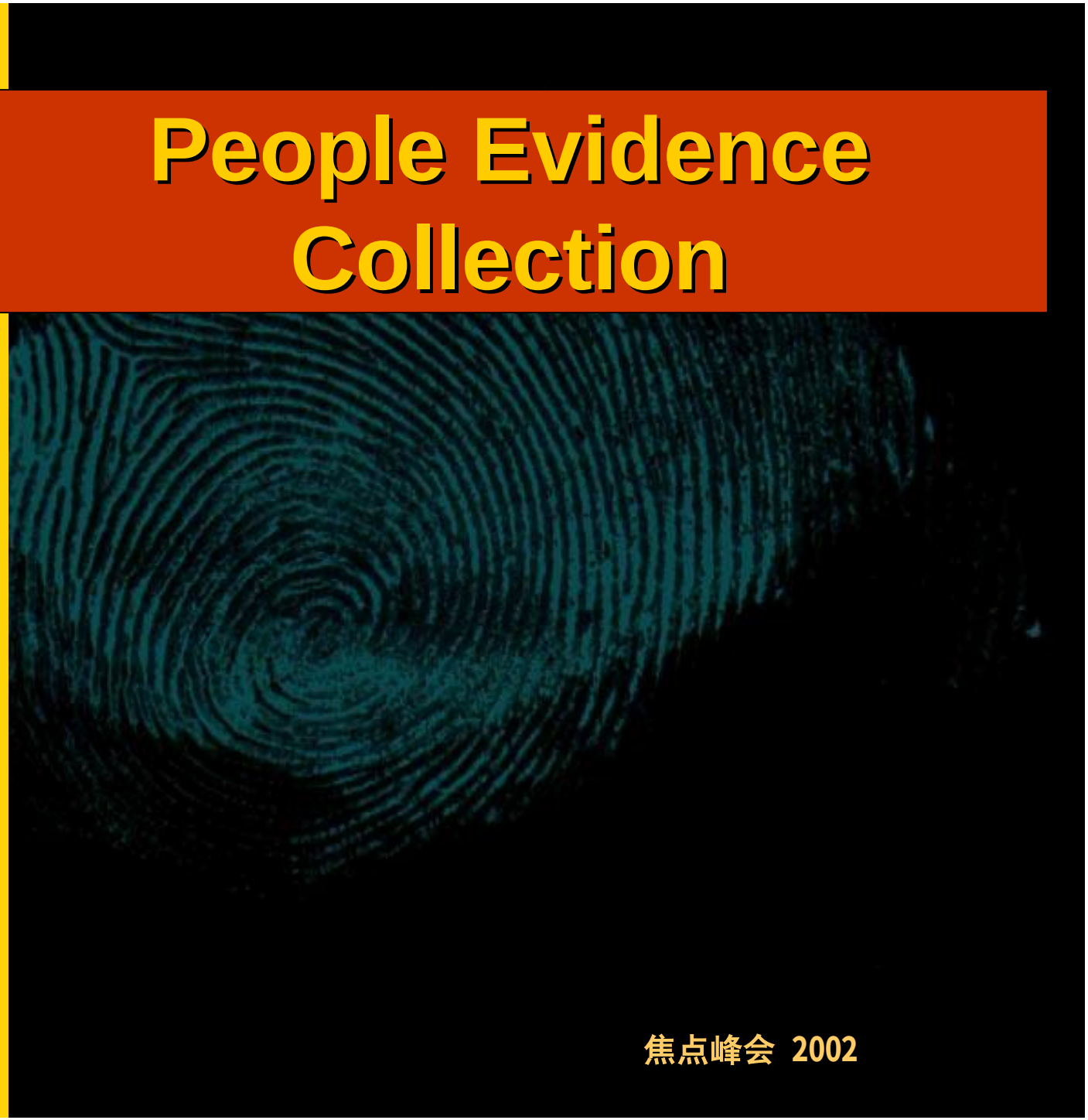
Data Collection Phase

- **Example output of mactime:**
  - Feb 09 02 13:25:20 642 m.. -rwxr-xr-x root/smtp root tmp/.new/patch.sol7
  - Feb 09 02 13:25:26 1226 m.. -rwxr-xr-x root/smtp root tmp/.new/patch.sol8
  - Feb 11 02 14:19:11 2441 m.. -rwxr-xr-x root/smtp root tmp/.new/p-engine
  - Feb 12 02 11:53:55 488 m.. -rwxr-xr-x root/smtp root tmp/.new/childkiller
  - Feb 12 02 18:53:18 4780 m.. -rwxr-xr-x root/smtp root tmp/.new/findkit
  - Feb 13 02 08:46:35 7328 m.. -rwxr-xr-x root/smtp root tmp/.new/heil
  - Feb 16 02 18:05:14 0 m.. -rw-r--r-- root/smtp root tmp/.new/cms
  - Feb 16 02 18:06:57 1003520 m.. -rw-r--r-- root/smtp root tmp/.new/newkit.tar
  - Feb 16 02 18:08:39 1024 m.. drwxr-xr-x root/smtp root tmp/.new
  - Mar 03 02 19:49:11 840936 m.. -rwxr-xr-x ronnie 100 tmp/eggdrop/eggdrop-1.6.8

Data Analysis Phase

- **Hard Part. Use your intelligent. Most time consuming part**
- **Do not always believe the data you collected, there maybe some trick and trap set up by your enemy**
- **Analyze 'tar' or compress file**
- **Analyze deleted data**
  - Use 'unrm' & 'lazarus'
  - Unrm /dev/dsk/c0t0d0s0 > $path/output
  - Lazarus –h output
  - Grep –il '$keyword' blocks/* > matchfile
  - Exhausting browsing thru the output block files

People Evidence Collection



安全焦点

www.Xfocus.org

焦点峰会 2002

Interview Technique

- **Why important:**
  - People, not just computer, are the most important facet of an IT investigation
  - Affect the effectiveness of Tech Investigation effort.

安全焦点
www.Xfocus.org

Interview Technique

- Target: To obtain complete and accurate information from all related people involved in the case

安全焦点
www.Xfocus.org

Interview Technique

- **Overall Speaking, the process is a study of human nature.**
- **1. Begin with building rapport:**
  - When rapport exist, your interviewee show unconscious mirroring of your new posture.
  - Rapport build thru:
    - Sit down with interviewee in a more quiet and private place
    - Speak slowly and softly (take note and ask interviewee to response slow)
    - Keeping a calm professional attitude
    - Dress more looking like your anticipated interviewee

安全焦点
www.Xfocus.org

Interview Technique

- **2. Rephrasing the question in just the right manner**
  - Visually: drawing type
  - Auditory type
  - Kinesthetic (feeling) type (hands-on type)

安全焦点
www.Xfocus.org

Interview Technique

- **3. Drill Down & Wide-Eyed**
  - 'showme'
  - It is not important what investigator know, it is important to document what the interviewee knew
  - Use their characteristic of 'show off'
- **4. Be prepared with strategy to identify and overcome deceptive interviewee**

安全焦点
www.Xfocus.org

Case Study

安全焦点
www.Xfocus.org

焦点峰会 2002

Case Study

- **Case Background**
  - Public Service Internet Server Hack-in
  - Detected by SA while hacker deleting all files ‘rm –rf /*’
  - Case Investigation started 6 months after???

Case Study

- **Investigation Process:**
  - Interview
    - Rapport
      - No authority while interview
      - Connection with same people
    - ‘feeling type’ interviewee
  - 3-phases technical investigation
    - Clone disk
    - Coroner toolkit to collect data
    - Data analysis, events correlation

安全焦点
www.Xfocus.org

Case Study

- **Investigation Target:**
  - What is the motive of the hacking?
    - Eggdrop to build base
    - Non-usable system – motive for destruction action.
  - Who is the hacker?
    - Intrusion time analysis
    - Hacking tools used: Solaris rootkit
  - How did the hacker get in?
    - O/S weakness
    - Application weakness
    - Network weakness

安全焦点
www.Xfocus.org

Case Study

- **Some Thought**
  - Most hacker will start their attack from a system in other country which result in time delaying and obstacle in investigation
  - Effective cyber crime investigation need involve insider (hacker), or Internet intelligent centre (honeypot, honeynet)

安全焦点
www.Xfocus.org

Thank You!

安全焦点
www.Xfocus.org

焦点峰会 2002