Forensics & Anti- Forensics

YingJian Wang

Casper@xfocus.org

2007-11-15

Who Am I ?

- The Orgenizer of XCon
- The Founder of XFocus Team
- The CEO of HYXA Science Techonlogy Co., Ltd
- Sr. Researcher of Institute for Internet Behavior, Tsinghua University
- ……

Agenda

- Forensics
  - Demo : File Slack and Delete File
  - Demo : Link File Analyse
  - Demo : USB Removal Storage Analyse
- Anti-Forensics
- Forensics in Hack
- What is our problems that we had Solved

Presentation Attention

- Clue Relationship Analyse
- Technical details
- Technology extend

What do the Forensics do?

- Find more file about your case
- Find the relationships between file and file
- Let the suspect can NOT deny
- ……

Forensics Process

- Get Evidence
  - Software:DD, Ghost, Encase, FTK ……
  - Hardware:DriveLock, Logicube MD5 & Sonix, UltraBlock, Solo3 ……
- Analyse Evidence
  - Data Recovery
  - File Check (Find, Encrypt, Signature…)

Forensics & Investigation

- What is it different with Forensics and Inverstigation ?
  - Forensics:
    - We had deduce who is the suspect , now need prove it is him.
    - We know what will be found (keyword…).
  - Inverstigation:
    - We don’t know who is the suspect , we need find some clues
    - We need check every file by possible file time, file format etc .

Forensics Tools

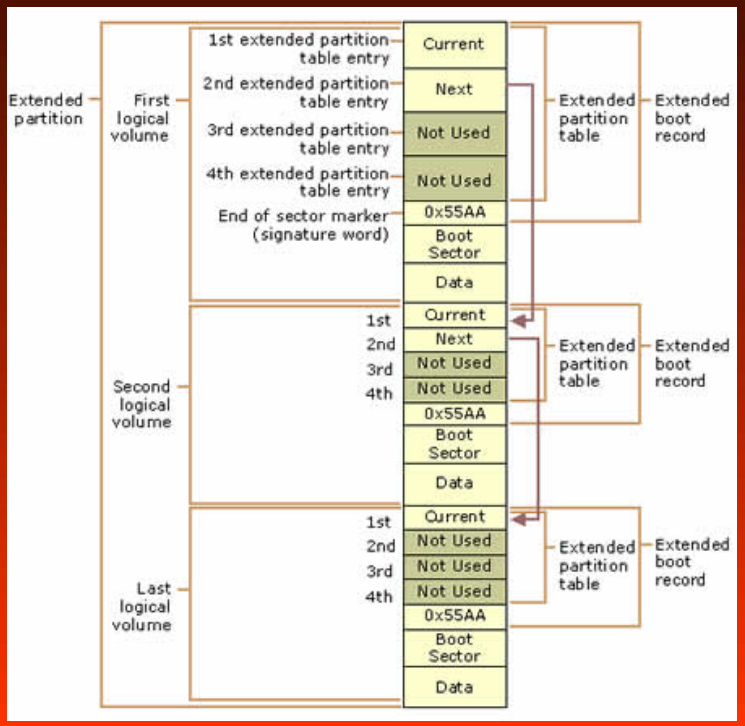
- Business Software:
  - EnCase, Forensics ToolKit, Fact-Based Investigation, MacForensicsLab.....
- Free Software:
  - DD, WinAudit, Fau, Nigilant32, Helix.....

3 Parts

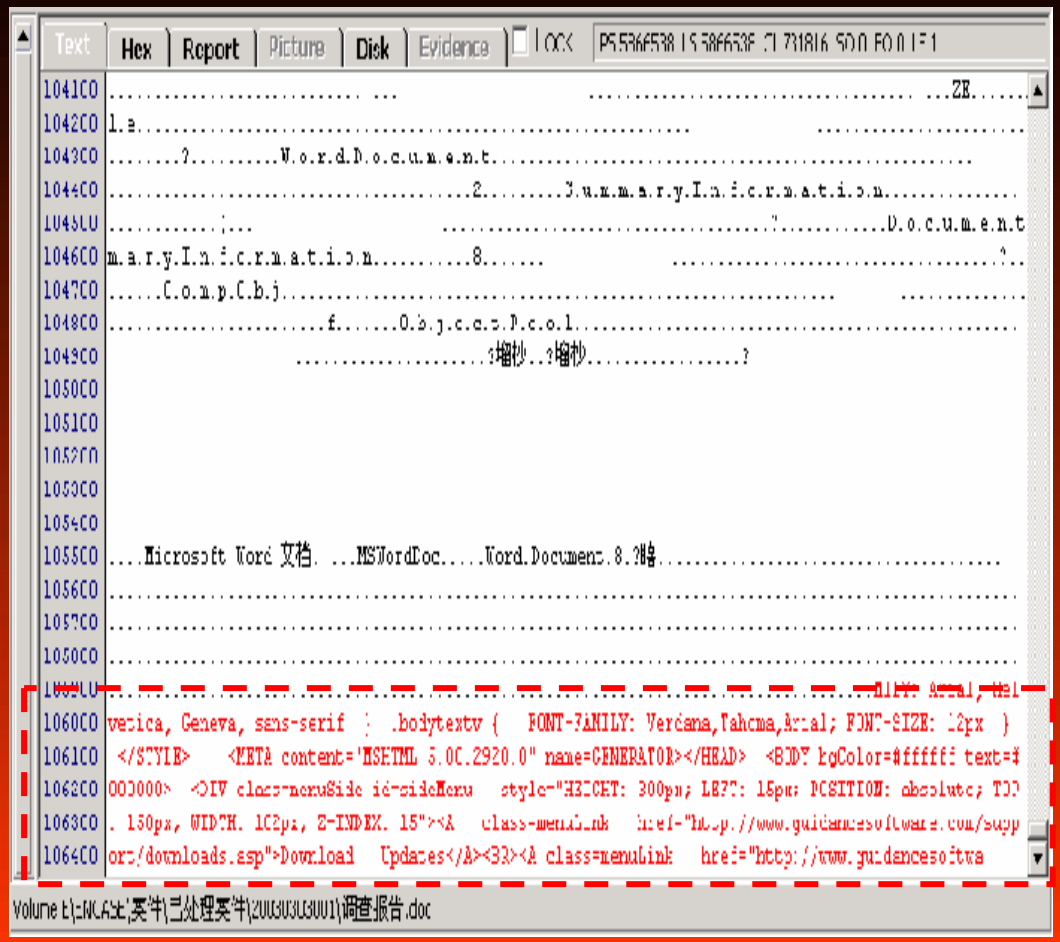
- Data Recovery & Searches
- Application & System log (File & Registry)
- Removable Storage

Data Recovery & Searches

- Everybody know how about delete a file & format a vol can be recoveried
- But After Disk defragment ?
  After format and Install new OS ?
- Yes, we can find some infor yet



File Slack



Logistic Size

Physical Size
2K

File Slack

Demo

- Internet Access Check :

  Background: Some Department ‘s computer only access intranet or don’t connect any computer.

  Intention: Check if access lawless net

  Method: Find http , ftp , cookie …

Application & System log

- Log File : *.evt *.log etc ...
- For example:
  - AOL Messager

    %Windows%\aim95*.dat, *.tmp
  - Acrobat:
    HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\xxxx\AVGeneral

    HKEY_CURRENT_USER\Software\Adobe\Acrobat\xxxx\Weblink\xxxx

Application & System log

- Google Toolbar

  HKEY_CURRENT_USER\Software\Google\NavClient\1.0, 1.1

  %AppData%\Google\Local Search History\google*web.w
- Cute ftp

  %ProgramFiles%\GlobalSCAPE\CuteFTP\sm.dat , sm.bak

  %ProgramFiles%\GlobalSCAPE\CuteFTP\log

Demo: Link File Analyse

- Link File relate to target object including:
  - Files
  - Applications
  - External drives
  - Printers
  - Folders

Inside the Link File

- The Created, accessed and last written time of the object
- Name
- Full path of object
- Volume lable
- Volume ID
- ……

Demo: USB Removal Storage Analyse

- USB Thumb Drive Process
  - Review SetupAPI.log
    - Section header for date and time of install
    - Device manufacturer and name
    - Device unique ID
  - Review Registry Entries
    - USBstor Key
    - Subkey for device name uniqueID & ParentID Prefix
    - Mounted Devices key
    - To map dos Device entry to ParentID Prefix
  - Review VolumeID
    - Physical drive volume ID from volume boot record
    - Link File

Anti-Forensics

- Wipe can reply all Host Forensics Tools
- Counterfeit Evidence
- Chicanery : If you want to hack, you can make a been hacked environment.
- When you can’t wipe log , you might let forensics become very complex and very difficult
- If you are hacking a honeypot and 3 administrators are looking anything , how to do?

Forensics in Hack

- By Forensics Tools, we can recovery and find more file quickly and exact
- We can get more information about administrator, enlarge hack harvest
- Data Analyse

Our Problem

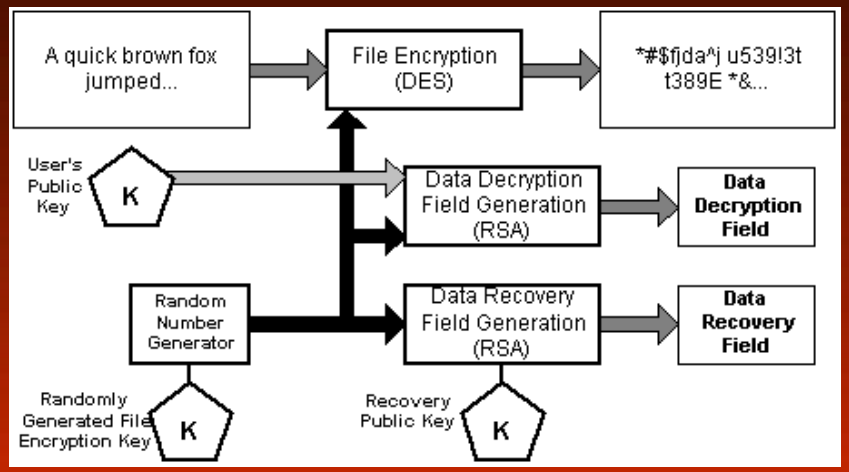
- We can touch the target machine , but we don’t have the user password
  - We want to know “*******” Password
  - We want to See EFS file content
  - We want to know password in DPAPI
    - MSN, Outlook, FTP, IE Saved Password .....
  - We want to know the SAM password
  - .....

Done

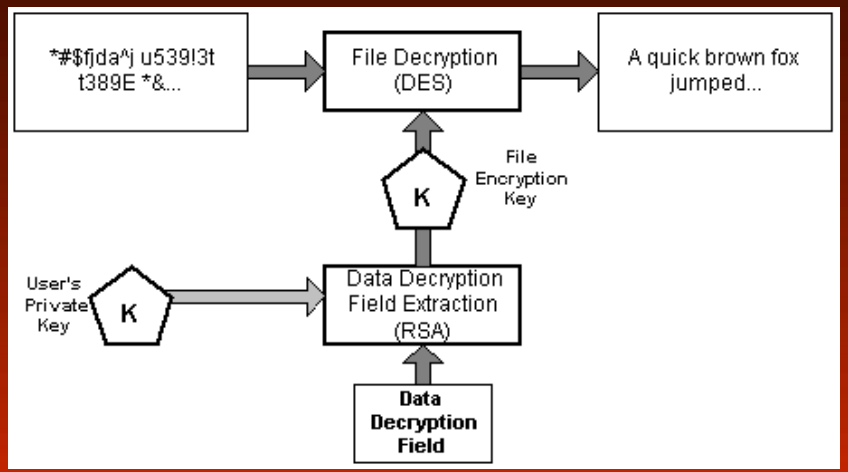
- We can crack SAM password to ClearText by P4 2.8G & Memory 1G
  - From SAM, SamDump, Password Hash
  - Lowercase+Capital+Digital+Symbol
    - Ciphertext Space is 62^n (n is passwd length)
    - If n=14, we need maximal 3 mins maximum
  - Lowercase+Capital+Digital
    - Ciphertext space is 97^n (n is passwd length)
    - If n=14, we need 40 mins maximum

Done

- EFS had been cracked.



EFS Encryption



EFS Decryption

Done

- We can get ClearText or HashText
  - We can log on windows system
  - We can check EFS file
  - We can put the axe in the helve
  - ……

Question ?

Thank you

- Thank you for your Patience!
- Thank you for Vangelis invite me !
- Sorry for my bad English !

Waitting For You!

- XFocus Team
  - http://www.xfocus.org
- XCon
  - XFocus Information Security Conference
  - http://xcon.xfocus.org
- We Research the Projects:
  - Vulnerability Discovery
  - Mobile Hack & Exploitation & Forensics
  - GSM/CDMA/WCDMA Security

감사합니다 !!!

poc2007@huayongxingan.com