重庆邮电大学
CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

# Extracting Text from Windows XP Memory Image

Long Chen, Lei Kang, Zhenxing Dong

Institute of Computer Forensics

Chongqing University of Posts and Telecommunications

2012.9

# Outline

- Background
- The characteristic of text
- Solution
- Conclusion

# Background

The challenge of computer forensics

- Massive data
- Lack of some important data
- Lost  everything in some cases ?

# Background

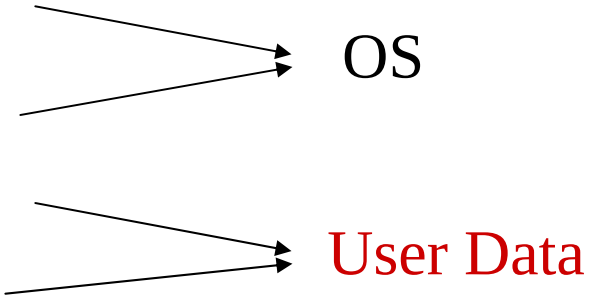
Memory forensics

- Registry
- Processes and threads
- Network connection
- Password
- Web
- ……

# Related works and Goal

- Related works

  Processes and threads
  Network connection
  Command line
  Clipboard




Problem Here to reconstruct the basic scene

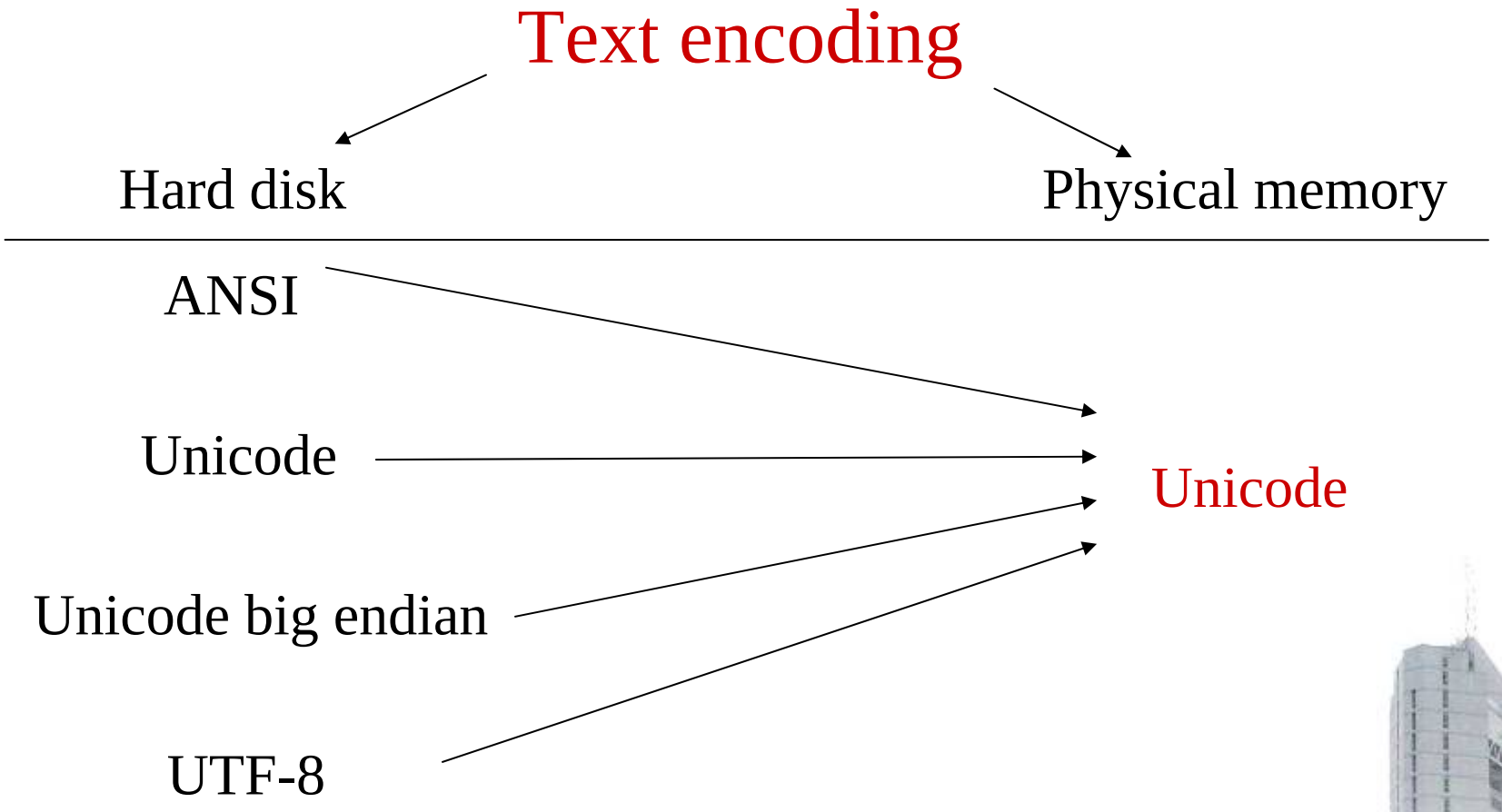
- Text is easy to explain, Helpful information

  At first, Considering the text file

# Outline

- Background
- The characteristic of text
- Solution
- Conclusion

# The characteristic of text

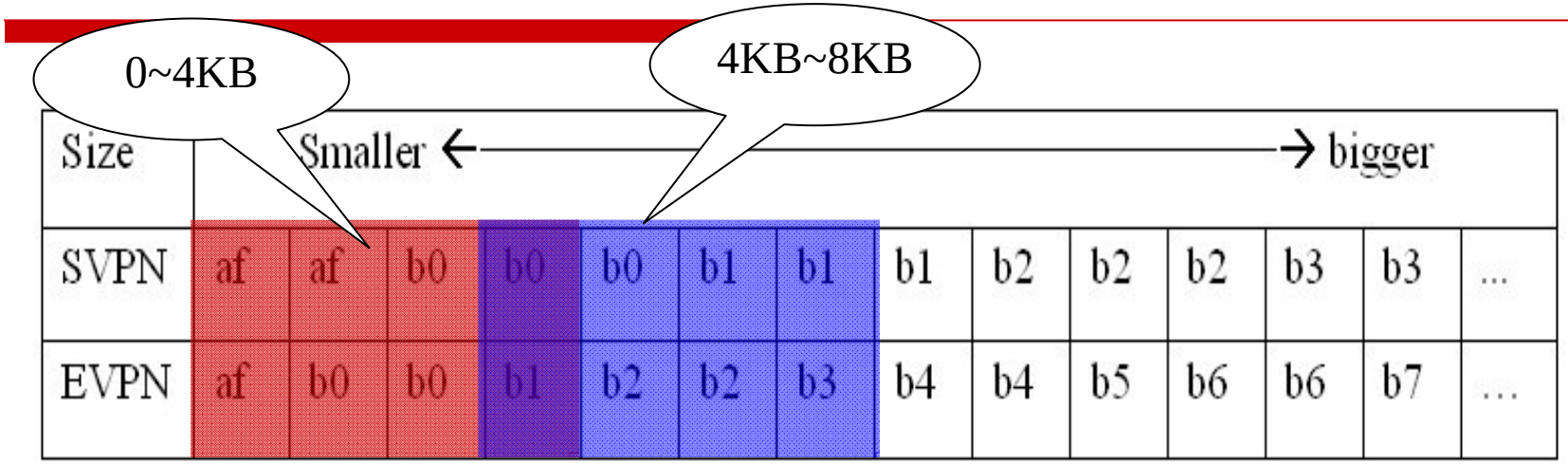





# Outline

- Background
- The characteristic of text
- Solution
- Conclusion

# Solution： virtual pages




All text's virtual page number must be in the interval [a,b], where

$$a = 0xae + \lfloor m/4KB \rfloor$$

$$b = 0xaf + \lfloor m/4KB \rfloor * 2$$

# Solution Flags for locating …

- The number of characters

The number of characters of the text is stored with four bytes in the virtual page 0xaa, and can be located with a flag "0xffffffff".

- The starting position **special flag**

A 12 bytes flag"0x010004002e 00740078007400" exists in front of the starting position of text.

# Solution： EPROCESS and KPROCESS

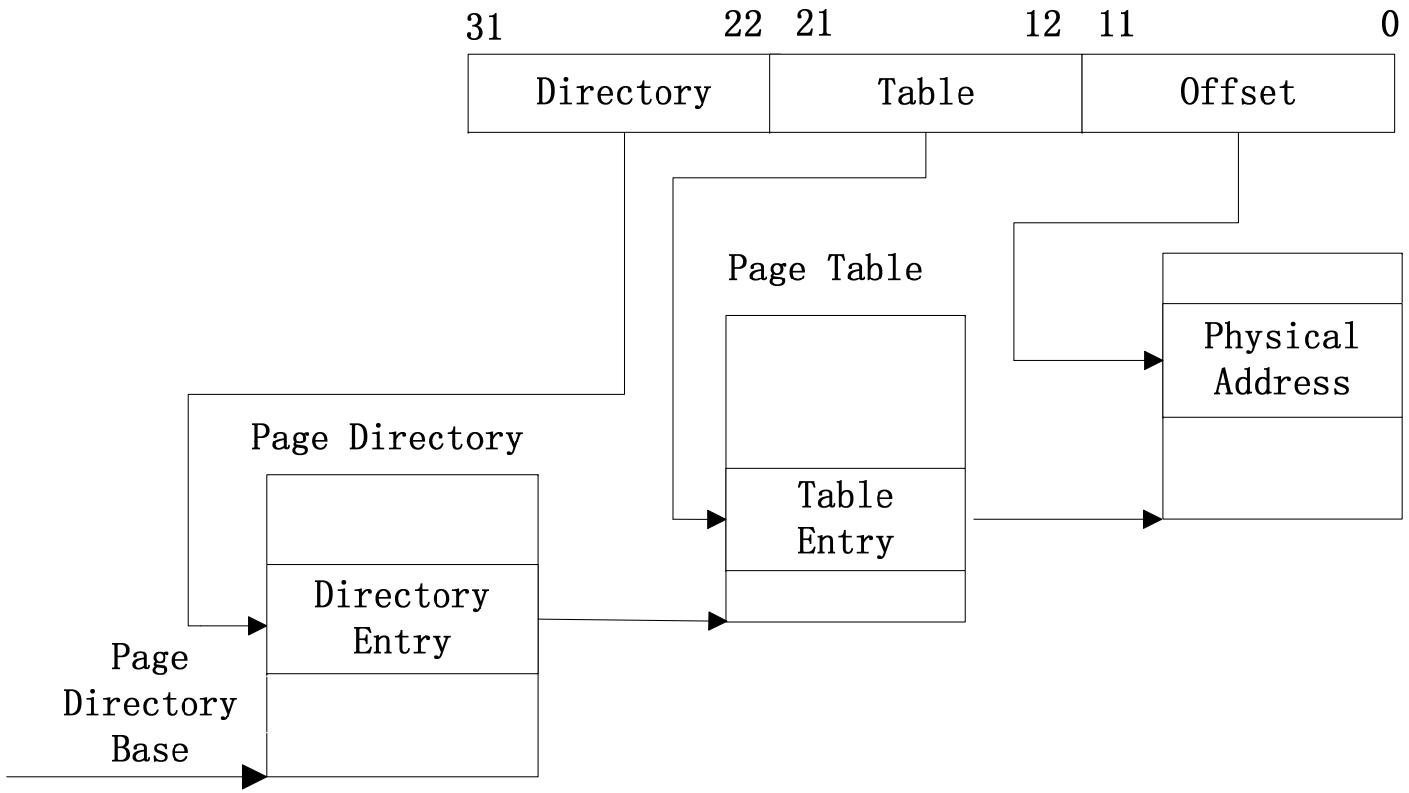
| +0x000 Pcb : _KPROCESS |
| --- |
| … |
| +0x078 ExitTime : _LARGR_INTEGER |
| … |
| +0x174 ImageFileName :[16]UChar |
| … |
| +0x1b0 Peb :Ptr32_PEB |
| … |
| +0x24c ExitStatus : Int4B |
| … |
| +0x258 Cookie : Int4B |

EPROCESS

| +0x000 Header :_DISPATCHER_HEADER |
| --- |
| … |
| +ox018 :DirectoryTableBase [2]Uint 4B |
| … |
| +0x06b ExecuteOptions UChar |

KPROCESS

# Solution： Address translation






# Solution： Process of Extracting text

- Searching _EPROCESS structure
- Getting the size of text
- Computing the interval of VPNs
- Getting the physical pages
- Searching the flag

  and Extracting the text

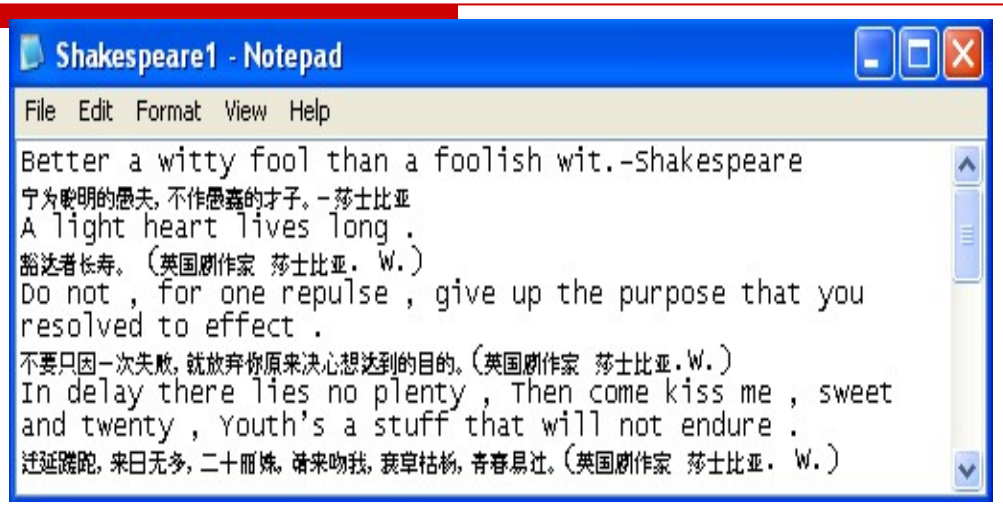
# Experiment

- Experimental environment

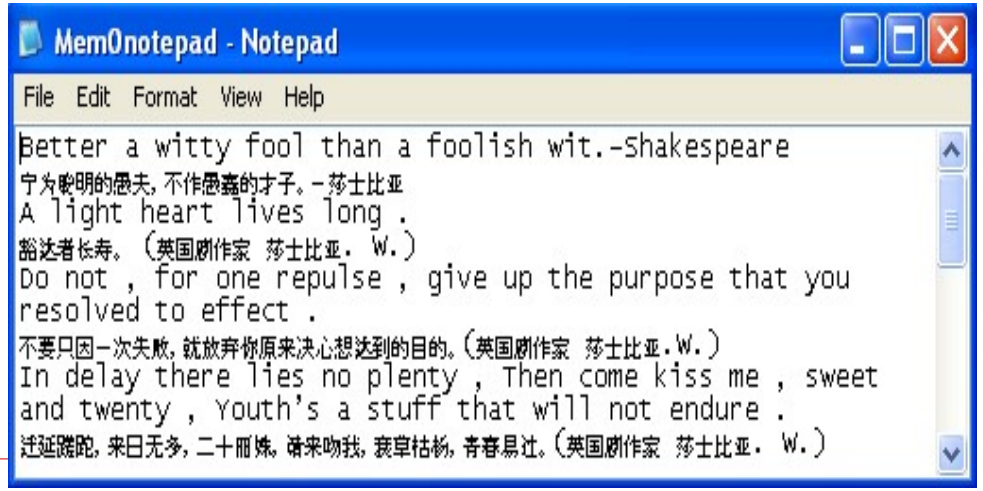
| | | |
|---|---|---|
| O S | : | XP (SP3 VOL) |
| Address extension | : | Noexecute |
| Memory | : | 512M |
| Image tool | : | DumpIt |

# Experiment

Original File




Generated File：






# Outline

- Background
- The characteristic of text
- Solution
- Conclusion

# Conclusion

- It can be reconstructed accurately
- Applicability

  Suitable to other versions of Windows XP in general with minor differences

# Thank you!

Q & A

Thanks for your attention！