Malware and Memory Forensics

I. Types of Analysis

a. Swap space analysis

b. Memory Analysis

c. Data acquisition as per RFC 3227

II. In-memory data

a. Current processes

b. Memory mapped files

c. Caches

d. Open Ports

III. Memory Architectural Issues

a. Data structures

b. Windows Objects

c. Processes

d. Handles

e. Pool-tag scanning

f. %SystemDrive%/hiberfil.sys

g. Page/Swap File

IV. Tools used

a. Using volatility

b. Dumpit.exe

c. hibr2bin

d. Win32dd

e. Win64dd

f. OSForensics

V. Registry in Memory