Computer Forensics

Marquette University 2017

Computer Forensics

- Reconstruction of events in a (or related to) an information technology system
  - Short History:
    - 1980s:
      - Massive use of PCs in businesses and homes
      - Computer as a witness appears
      - First instances of computer crime
    - 1990s:
      - Computer Forensics becomes a discipline
      - Specialized tools are developed
      - Processes for acquiring evidence are adopted
    - 2000s:
      - Computer Forensics becomes its own academic discipline
      - With remote storage and investigations

Computer Forensics

- Deployed in organizations
  - Reconstruction of abuses of IT resources
    - Intellectual property protection, Fraud detection, Litigation support
  - Reconstruction of intrusion incidents
    - What was affected?
    - Cleaning
  - Intrusion prevention

Computer Forensics

- Used by public order agencies
  - Majority of mayor crime involve computing devices
    - Cell phones, GPS, PC, Tablets

Computer Forensics

- IT system
  - Can be target of a crime
    - Intrusions, worms, virus, DoS, unauthorized changes to a database, …
  - Can be the instrument of a crime
    - Falsifying email, change of grades against pay, using google maps to plan crimes, …
  - Can obtain evidence of a crime
    - Communications, …

Evidence

- Computer Forensics evaluates and safeguards evidence
    - Needs to comply with the requirements of evidence handling
        - Character of an investigation can change during its lifetime
            - But mistreated evidence will not regain its value

Evidence

- In the US, forensics needs to use the scientific method
  - Needs to satisfy the Daubert criteria
    - Existence of standards and controls
    - Acceptance of methods by the scientific community
    - Peer-reviewed publications
    - Known error rate

Computer Evidence

- Character of IT evidence
    - Artifacts can be reproduced completely faithfully
        - Means that one can work with complete security with an exact copy of evidence
    - Recognized falsified evidence needs expertise
        - But is in general possible

Evidence

- Chain of custody
  - Preservation of evidence in a verifiable manner
  - Implies the use of verifiable tools
  - In practice, there is much destroyed evidence
    - Often by helpful system administrators

Computer Forensics

- Subdisciplines
  - Storage forensics and life system analysis
  - Network forensics
  - File and especially malware forensics

Computer Forensics

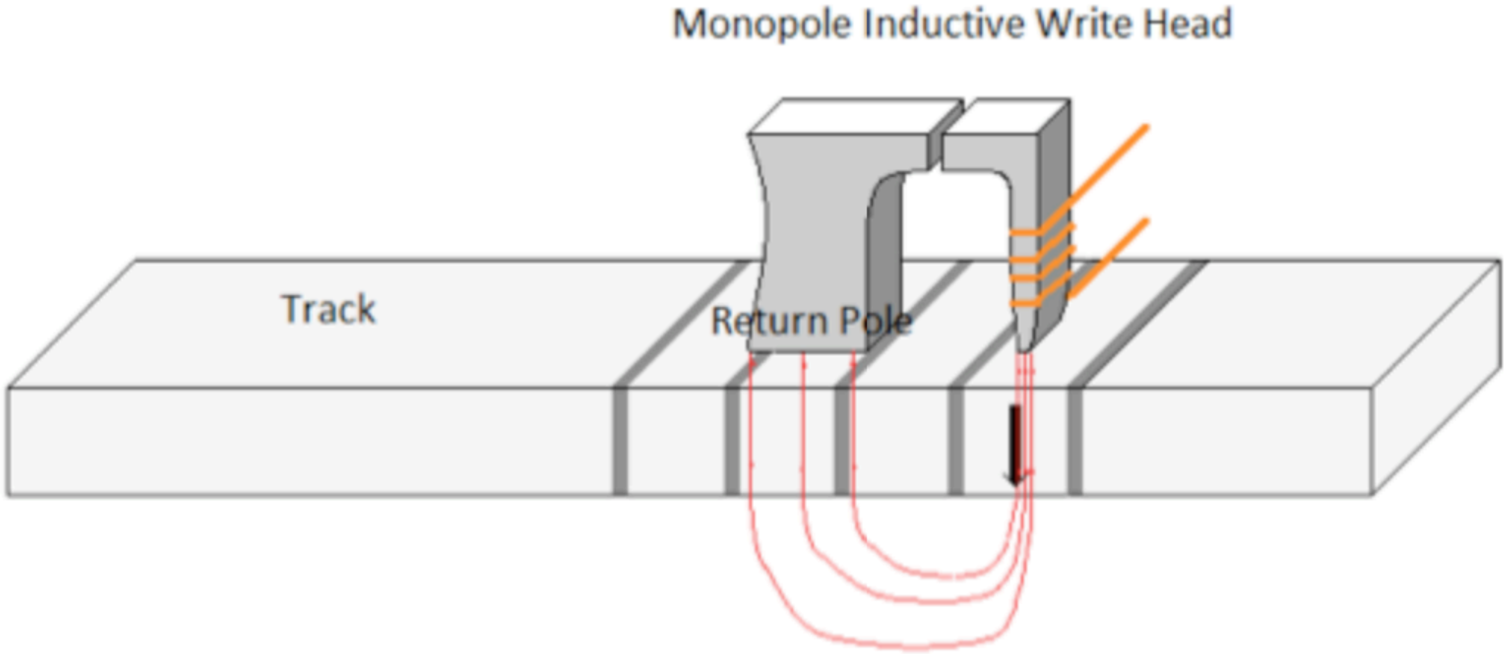
- Scheme of an investigation
  - Problem or incident triggers intervention
    - Preliminary identification of the goal of the investigation
  - Identification of potential evidence and its acquisition
  - Forensic Analysis of potential evidence
    - Requires refining the task and looking for more potential evidence
    - Interacting with the detective in charge or the decision makers
  - Presentation of the reconstruction of events and the evidence in a manner accessible to decision makers

Media Forensics

- Majority of data is stored on disks or flash memory
- Disks and flash memory have particular properties
- Stored in blocks / pages of 512B or 4KB

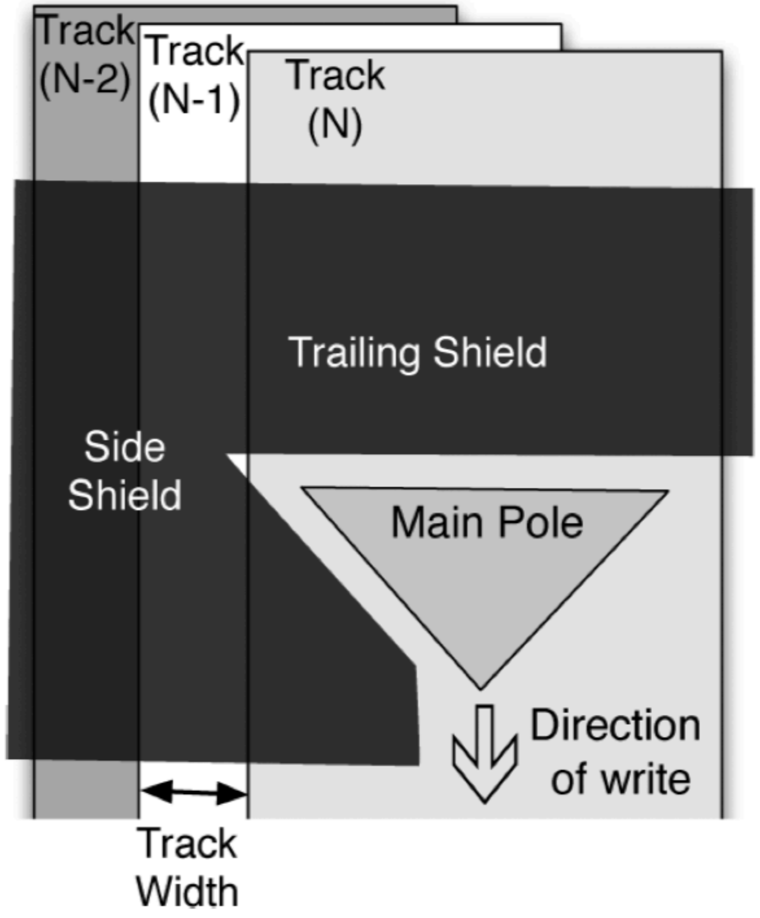
Media Forensics

- Disk properties
  - Disks have become smarter over the years
  - Write by magnetizing pattern on disk
  - In concentric tracks divided into sectors



Media Forensics

- Reading is done using the Giant Magneto-Resistive Effect
  - Latest capacity increases due to shingled writing
    - Overwrites parts of previously written track



Media Forensics

- Disk Drive Characteristic
  - Only writes complete blocks
  - Needs internal disk interface in order to restore data
    - Bits are encoding using a proprietary magnetic coding with in-built error detection and correction
    - Would need an electron microscope and the coding to even have a chance of recovering data
  - Disks do not need to erase data to overwrite a sector
  - Small chance of a disk having latent sector failures (sector cannot be read, e.g. because of an off-track write)

Media Forensics

- Only complete sectors are written
- File systems delete data by marking them as unread, but the data remains
- File system organizes data in unexpected ways: backups, revision control, copy on write, journaling file system, etc
- Disk drive behavior is not controlled by file system:
    - bad block replacement, optimizations, …
- To completely delete a file:
    - Overwrite sectors where file was stored
        - Called *wiping*
    - No longer need to worry about previous magnetic patterns not completely erased by an overwrite
    - Overwrite sectors where meta-data is stored
    - Or physically destroy the file

Media Forensics

- HDD
    - Have become more intelligent
        - Use sophisticated combined magnetic and error-correcting coding
        - Use write buffers
        - Use address translation because the traditional values for cylinder & sector do not have the best range
        - Even block numbers have to be translated
        - Can use timing tool to find out the real geometry

Media Forensics

- HDD access:
  - Now only possible through the disk controller
  - Block-based command allow true access to the data
    - But not to the magnetic patterns etc.

Media Forensics

- SSD
  - Use Flash Memory
    - Data organized in pages which are part of erase-blocks
    - SSD constantly moves used pages elsewhere to create empty erase-blocks
    - Erase-block is then erased
  - FTL: Flash Translation Layer
    - Internal outlay of data varies
    - View of data from outside the SSD stays the same

Media Forensics

- Evidence protection for HDD
  - Since HDD contents do not change without operations:
    - Can use a hash of all the contents in order to prove that there was no alteration
- Acquiring hard-drive for evidence
  - Use a write-blocker
    - Software or hardware
  - Make copy of disk
    - add one for the defense
  - Analyze the copy

NoWrite
FPU
Field Preview Unit
▼ Your Computer ▼

Forensic
UltraDock v4
wiebeTECH
PATA
SATA
4 Pin PWR
DC PWR
DC
eSATA
www.wiebetech.com

FireFly 800
Digital Intelligence
Pwr
WrBlk
Act

FireFly™ 800
Digital Intelligence
800/400
Bilingual
Pwr
WrBlk
Act
DC IN
+5V

Media Forensics

- Problems with acquiring a hard drive
  - Invisible partitions (no problem)
  - Host Protected Area (no problem for good software)
  - Device Configuration Overlay (no problem for good software)
- Even though people will tell you that you can data there

Media Forensics

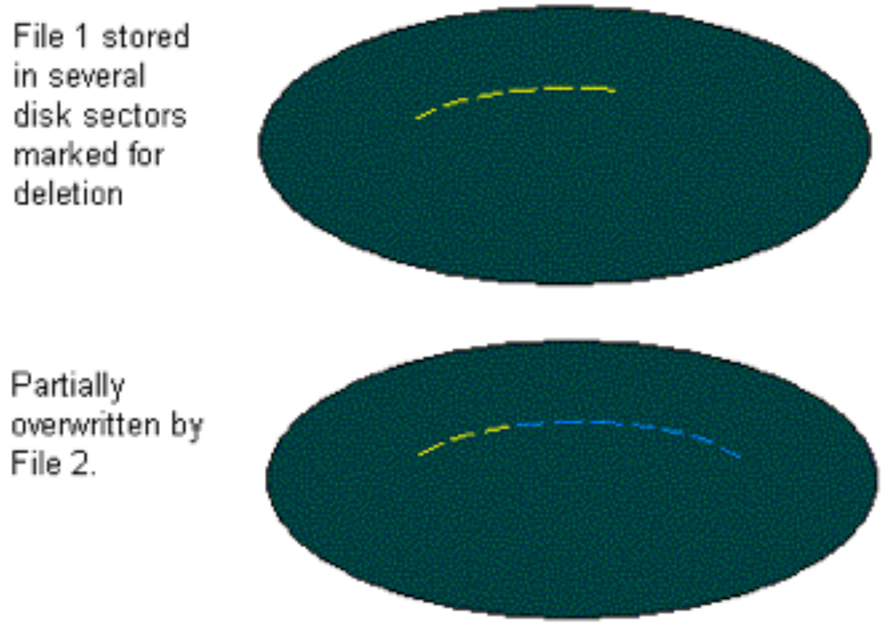
- SSD:
    - Since they change content the moment they have electricity:
        - Use strict evidence handling procedures to ensure that the SSD was not contaminated
        - Create a copy with write-blocker
            - But you can no longer prove that the copy is a true copy by hash or bitwise comparison

Media Forensics

- What can you do
    - User files
        - Temporary internet files
        - Registry contents
        - Files identified by keyword searches
            - E.g. look for social security numbers
        - Printer spooling files, images, etc.
        - Logs, prefetch files

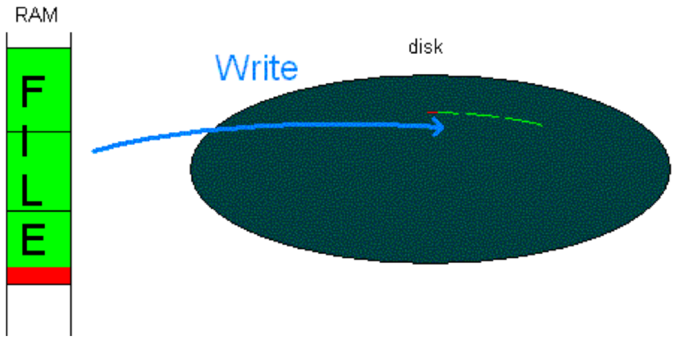
Media Forensics

- Deleted files
  - Are usually around
    - Information is in the file itself
    - And the metadata
  - Can be partially available
- RAM Slack

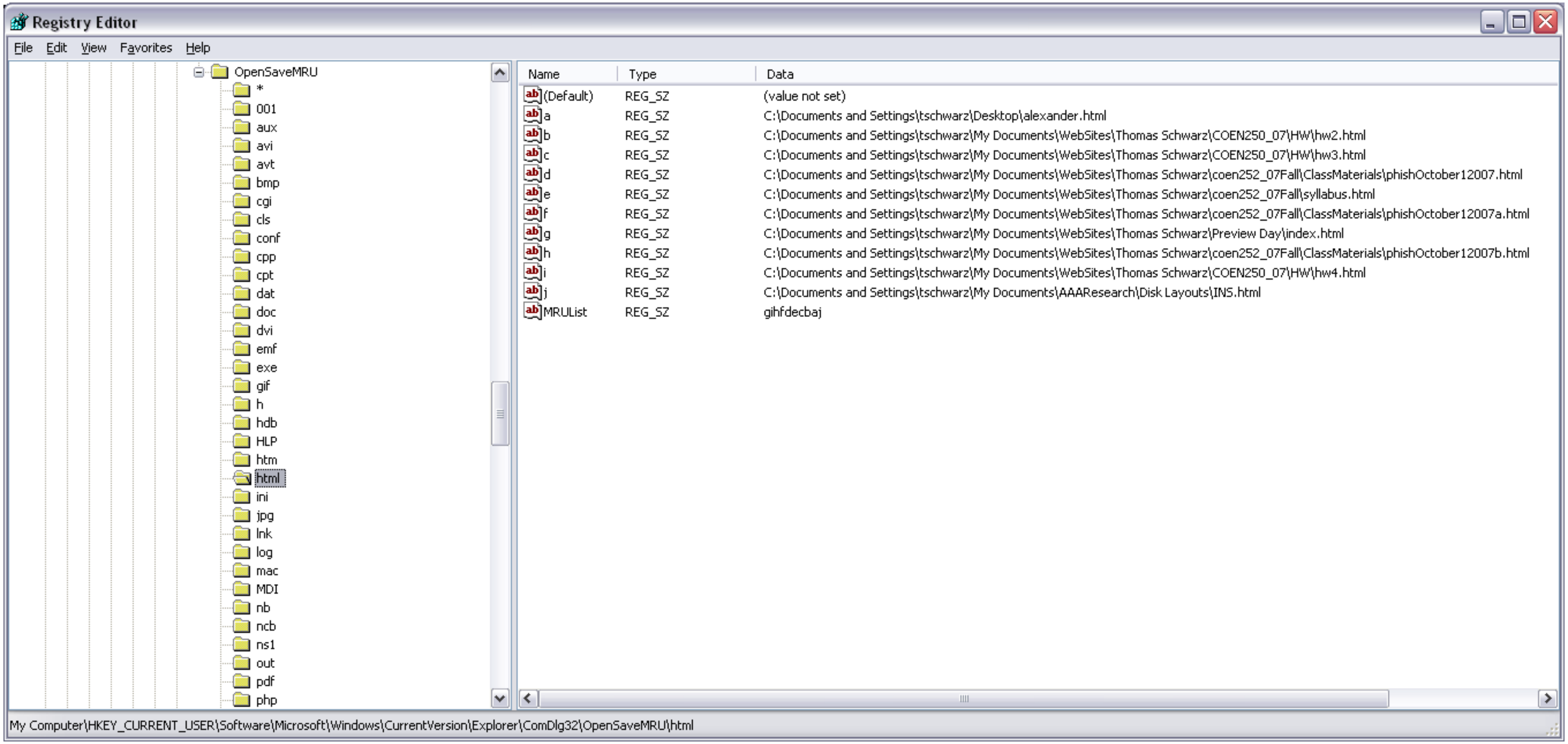


File 1 stored in several disk sectors marked for deletion

Partially overwritten by File 2.



Media Forensics

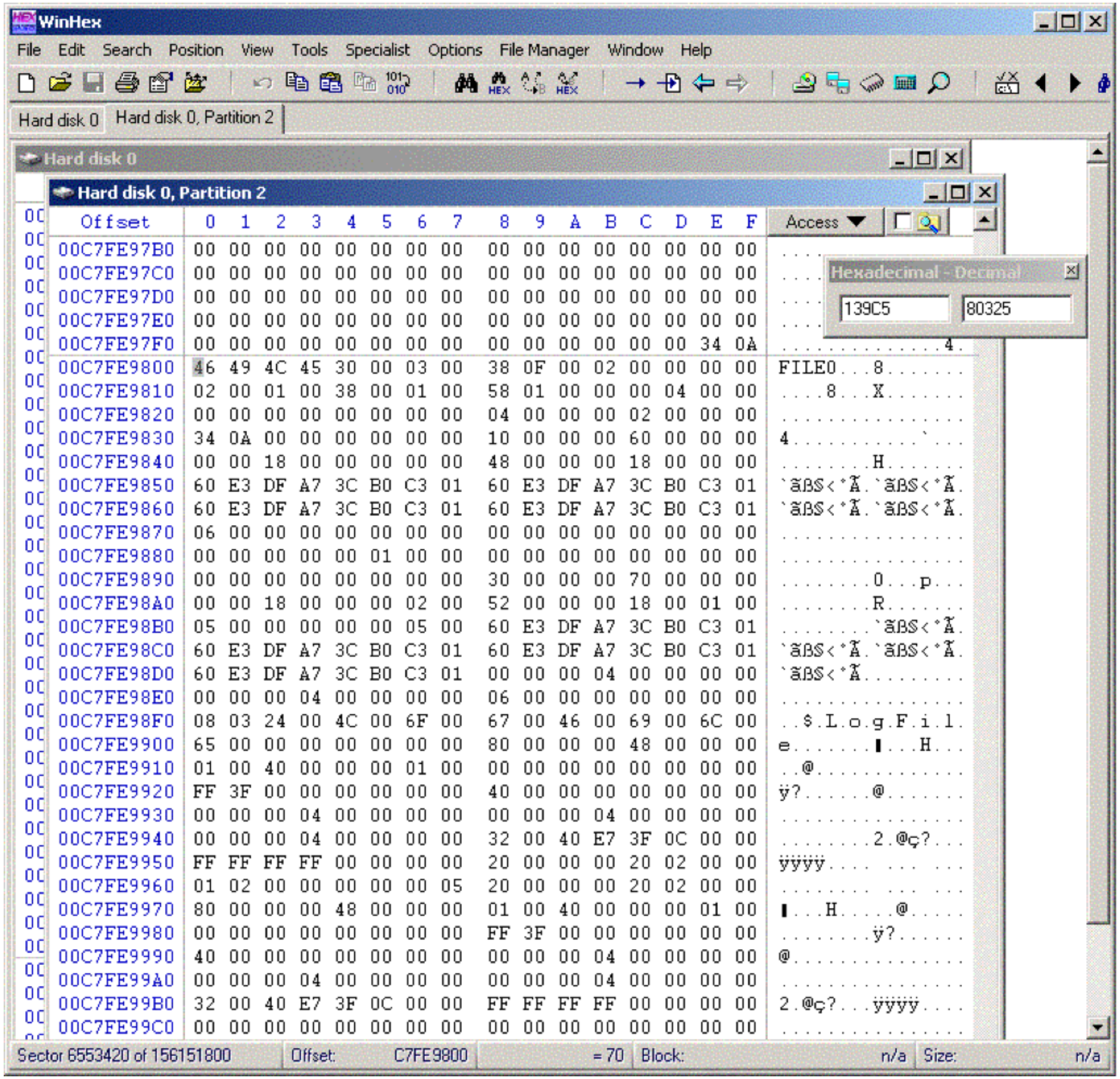


Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	C:\Documents and Settings\tschwarz\Desktop\alexander.html
b	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw2.html
c	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw3.html
d	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007.html
e	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\syllabus.html
f	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007a.html
g	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\Preview Day\index.html
h	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\coen252_07Fall\ClassMaterials\phishOctober12007b.html
i	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\WebSites\Thomas Schwarz\COEN250_07\HW\hw4.html
j	REG_SZ	C:\Documents and Settings\tschwarz\My Documents\AAAResearch\Disk Layouts\INS.html
MRUList	REG_SZ	gihfdecbaj

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\html

Media Forensics

- Metadata:
  - Note the time stamps

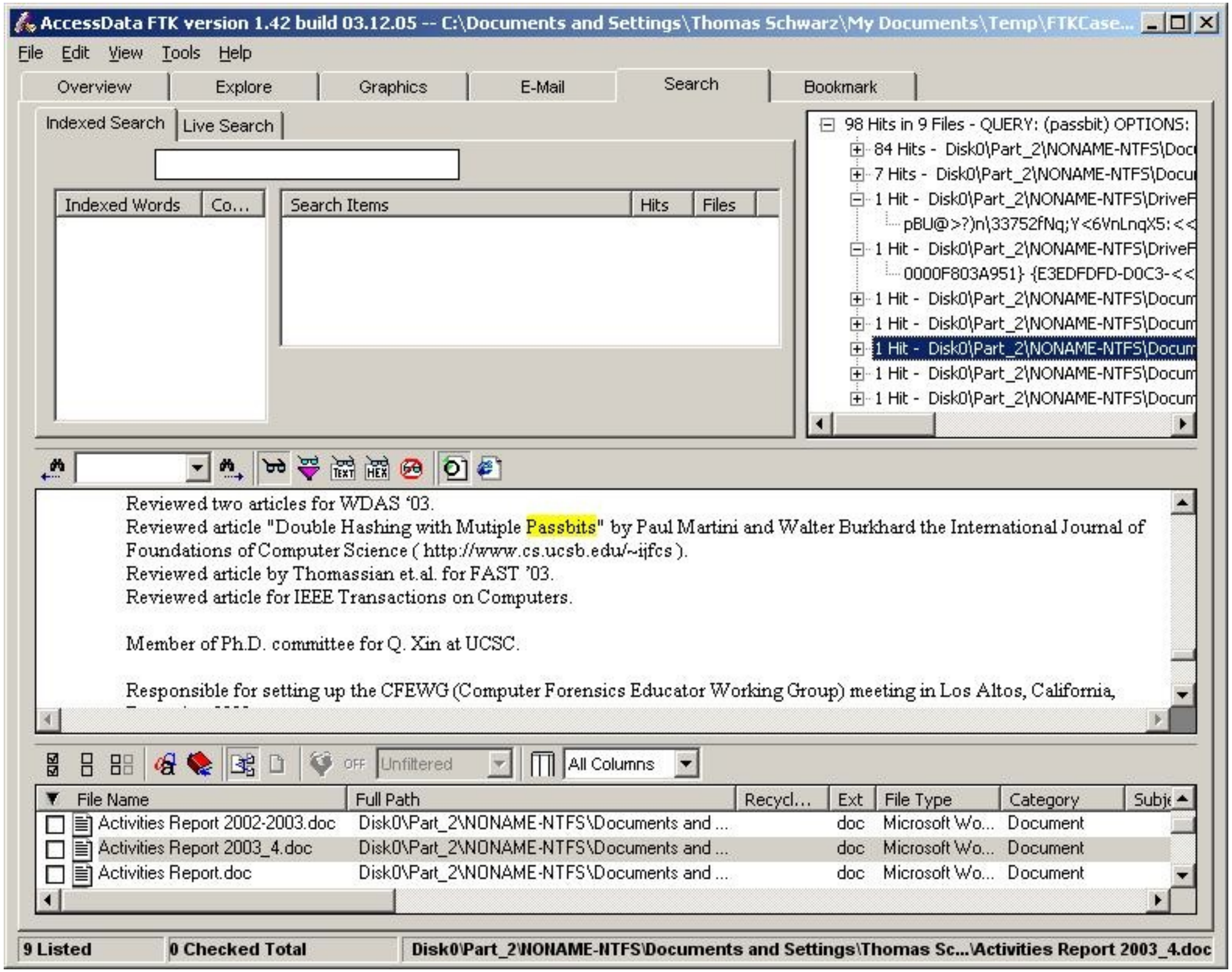

WinHex
File Edit Search Position View Tools Specialist Options File Manager Window Help
Hard disk 0
Hard disk 0, Partition 2
Access
Hexadecimal - Decimal

139C5 80325

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00C7FE97B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FE97C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FE97D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FE97E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FE97F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 34 0A  ..............4.
00C7FE9800  46 49 4C 45 30 00 03 00  38 0F 00 02 00 00 00 00  FILE0...8.......
00C7FE9810  02 00 01 00 38 00 01 00  58 01 00 00 00 04 00 00  ....8...X.......
00C7FE9820  00 00 00 00 00 00 00 00  04 00 00 00 02 00 00 00  ................
00C7FE9830  34 0A 00 00 00 00 00 00  10 00 00 00 60 00 00 00  4...........`...
00C7FE9840  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
00C7FE9850  60 E3 DF A7 3C B0 C3 01  60 E3 DF A7 3C B0 C3 01  `ãß§<°Ã.`ãß§<°Ã.
00C7FE9860  60 E3 DF A7 3C B0 C3 01  60 E3 DF A7 3C B0 C3 01  `ãß§<°Ã.`ãß§<°Ã.
00C7FE9870  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FE9880  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00C7FE9890  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00  ........0...p...
00C7FE98A0  00 00 18 00 00 00 02 00  52 00 00 00 18 00 01 00  ........R.......
00C7FE98B0  05 00 00 00 00 00 05 00  60 E3 DF A7 3C B0 C3 01  ........`ãß§<°Ã.
00C7FE98C0  60 E3 DF A7 3C B0 C3 01  60 E3 DF A7 3C B0 C3 01  `ãß§<°Ã.`ãß§<°Ã.
00C7FE98D0  60 E3 DF A7 3C B0 C3 01  00 00 00 04 00 00 00 00  `ãß§<°Ã.........
00C7FE98E0  00 00 00 04 00 00 00 00  06 00 00 00 00 00 00 00  ................
00C7FE98F0  08 03 24 00 4C 00 6F 00  67 00 46 00 69 00 6C 00  ..$.L.o.g.F.i.l.
00C7FE9900  65 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00  e.......▮...H...
00C7FE9910  01 00 40 00 00 00 01 00  00 00 00 00 00 00 00 00  ..@.............
00C7FE9920  FF 3F 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ÿ?......@.......
00C7FE9930  00 00 00 04 00 00 00 00  00 00 00 04 00 00 00 00  ................
00C7FE9940  00 00 00 04 00 00 00 00  32 00 40 E7 3F 0C 00 00  ........2.@ç?...
00C7FE9950  FF FF FF FF 00 00 00 00  20 00 00 00 20 02 00 00  ÿÿÿÿ............
00C7FE9960  01 02 00 00 00 00 00 05  20 00 00 00 20 02 00 00  ................
00C7FE9970  80 00 00 00 48 00 00 00  01 00 40 00 00 00 01 00  ▮...H.....@.....
00C7FE9980  00 00 00 00 00 00 00 00  FF 3F 00 00 00 00 00 00  ........ÿ?......
00C7FE9990  40 00 00 00 00 00 00 00  00 00 00 04 00 00 00 00  @...............
00C7FE99A0  00 00 00 04 00 00 00 00  00 00 00 04 00 00 00 00  ................
00C7FE99B0  32 00 40 E7 3F 0C 00 00  FF FF FF FF 00 00 00 00  2.@ç?...ÿÿÿÿ....
00C7FE99C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Sector 6553420 of 156151800 | Offset: C7FE9800 | = 70 | Block: n/a | Size: n/a

Media Forensics


AccessData FTK version 1.42 build 03.12.05 -- C:\Documents and Settings\Thomas Schwarz\My Documents\Temp\FTKCase...
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Indexed Search
Live Search
Indexed Words
Co...
Search Items
Hits
Files
OFF
Unfiltered
All Columns

```
98 Hits in 9 Files - QUERY: (passbit) OPTIONS:
  84 Hits - Disk0\Part_2\NONAME-NTFS\Doc
  7 Hits - Disk0\Part_2\NONAME-NTFS\Docu
  1 Hit - Disk0\Part_2\NONAME-NTFS\DriveF
    pBU@>?)n\33752fNq;Y<6VnLnqX5:<<
  1 Hit - Disk0\Part_2\NONAME-NTFS\DriveF
    0000F803A951} {E3EDFDFD-D0C3-<<
  1 Hit - Disk0\Part_2\NONAME-NTFS\Docum
  1 Hit - Disk0\Part_2\NONAME-NTFS\Docum
  1 Hit - Disk0\Part_2\NONAME-NTFS\Docum
  1 Hit - Disk0\Part_2\NONAME-NTFS\Docum
  1 Hit - Disk0\Part_2\NONAME-NTFS\Docum
```

Reviewed two articles for WDAS '03.
Reviewed article "Double Hashing with Mutiple Passbits" by Paul Martini and Walter Burkhard the International Journal of Foundations of Computer Science (http://www.cs.ucsb.edu/~ijfcs).
Reviewed article by Thomassian et.al. for FAST '03.
Reviewed article for IEEE Transactions on Computers.

Member of Ph.D. committee for Q. Xin at UCSC.

Responsible for setting up the CFEWG (Computer Forensics Educator Working Group) meeting in Los Altos, California,

File Name	Full Path	Recycl...	Ext	File Type	Category	Subj
□ Activities Report 2002-2003.doc	Disk0\Part_2\NONAME-NTFS\Documents and ...		doc	Microsoft Wo...	Document	
□ Activities Report 2003_4.doc	Disk0\Part_2\NONAME-NTFS\Documents and ...		doc	Microsoft Wo...	Document	
□ Activities Report.doc	Disk0\Part_2\NONAME-NTFS\Documents and ...		doc	Microsoft Wo...	Document	

9 Listed | 0 Checked Total | Disk0\Part_2\NONAME-NTFS\Documents and Settings\Thomas Sc...\Activities Report 2003_4.doc

Media Forensics

- File and OS System Metadata
  - Registry
  - Inode numbers are assigned in order

Media Forensics

- Anti-forensics
  - Wiping software
  - Time stamp changer
  - …

New challenges in Media Forensics

- Move to SSD as standard storage system for individual devices
- Storage in the cloud
  - Usually strongly encrypted
  - Larger difficulty of obtaining warrants

Network Forensics

- Relies on
  - Logs
    - Authentication Services
    - Emails
    - Intrusion Detection Systems
  - Rarely on directly intercepted data

Network Forensics

- Email investigations
  - Email consists of message proper and headers
    - Headers are added at each step of the way
    - Use inconsistencies to find evidence for forging
  - Principal method:
    - Verify details of each header
      - IP address - whois
      - Timestamps (beware of time zone changes and non-synchronized clocks)

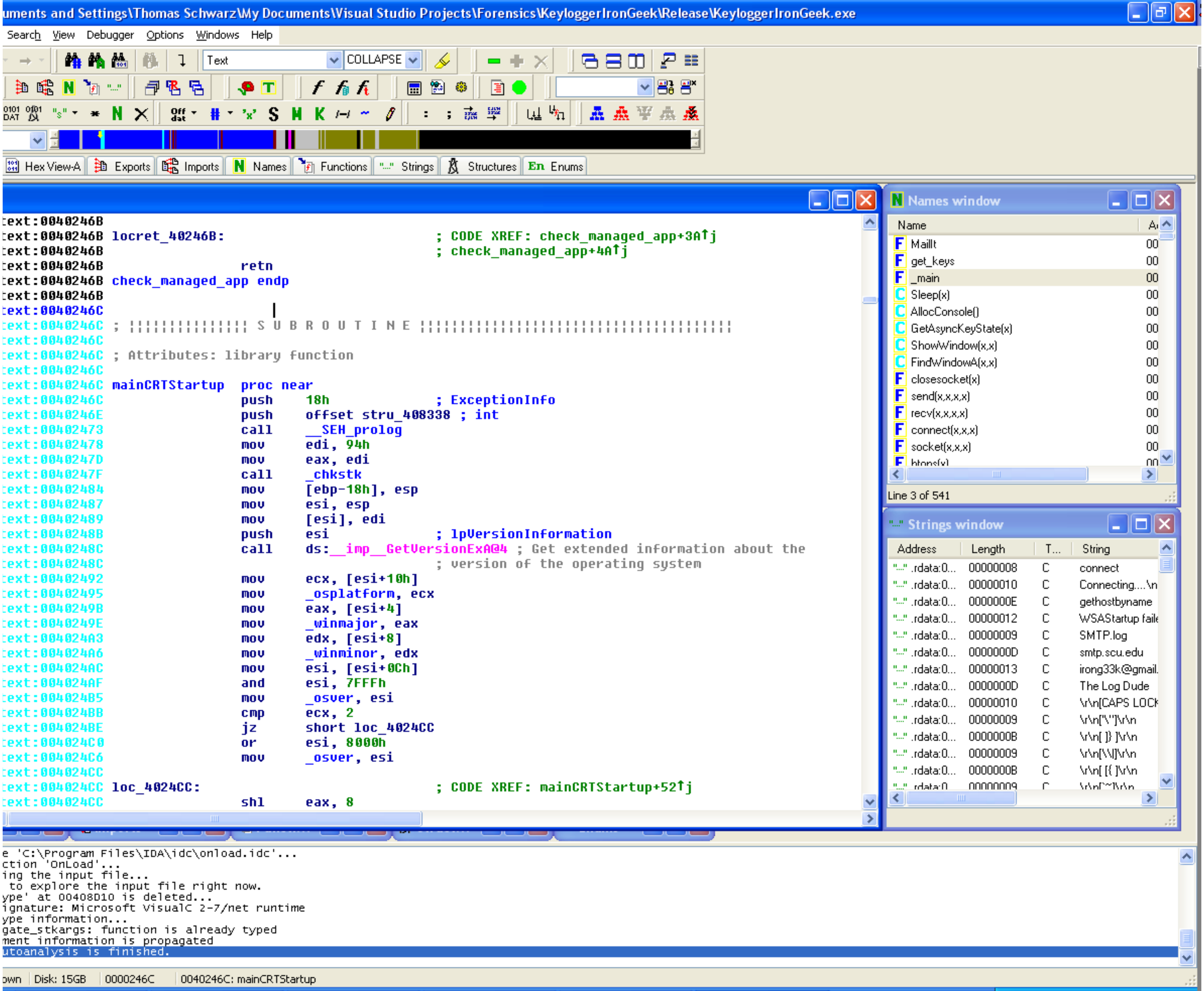
Malware Forensics

- Malware Forensics
  - Find malware and analyze its functionality
    - Example: Code Red

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

Malware Forensics

- Reverse Engineering
  - Use deassembler to obtain a more readable version
  - Use debuggers (Ollydbf, Softice, IDA-Pro)
  - Run programs in a sandbox and monitor access to file systems
    - Filemon, TCPView, RegMon, ProtMon, WinObj, Process Explorer


uments and Settings\Thomas Schwarz\My Documents\Visual Studio Projects\Forensics\KeyloggerIronGeek\Release\KeyloggerIronGeek.exe
Search View Debugger Options Windows Help
Text
COLLAPSE
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

```
ext:0040246B
ext:0040246B locret_40246B:                        ; CODE XREF: check_managed_app+3A↑j
ext:0040246B                                       ; check_managed_app+4A↑j
ext:0040246B                 retn
ext:0040246B check_managed_app endp
ext:0040246B
ext:0040246C
ext:0040246C ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
ext:0040246C
ext:0040246C ; Attributes: library function
ext:0040246C
ext:0040246C mainCRTStartup  proc near
ext:0040246C                 push    18h             ; ExceptionInfo
ext:0040246E                 push    offset stru_408338 ; int
ext:00402473                 call    __SEH_prolog
ext:00402478                 mov     edi, 94h
ext:0040247D                 mov     eax, edi
ext:0040247F                 call    _chkstk
ext:00402484                 mov     [ebp-18h], esp
ext:00402487                 mov     esi, esp
ext:00402489                 mov     [esi], edi
ext:0040248B                 push    esi             ; lpVersionInformation
ext:0040248C                 call    ds:__imp__GetVersionExA@4 ; Get extended information about the
ext:0040248C                                         ; version of the operating system
ext:00402492                 mov     ecx, [esi+10h]
ext:00402495                 mov     _osplatform, ecx
ext:0040249B                 mov     eax, [esi+4]
ext:0040249E                 mov     _winmajor, eax
ext:004024A3                 mov     edx, [esi+8]
ext:004024A6                 mov     _winminor, edx
ext:004024AC                 mov     esi, [esi+0Ch]
ext:004024AF                 and     esi, 7FFFh
ext:004024B5                 mov     _osver, esi
ext:004024BB                 cmp     ecx, 2
ext:004024BE                 jz      short loc_4024CC
ext:004024C0                 or      esi, 8000h
ext:004024C6                 mov     _osver, esi
ext:004024CC
ext:004024CC loc_4024CC:                           ; CODE XREF: mainCRTStartup+52↑j
ext:004024CC                 shl     eax, 8
```

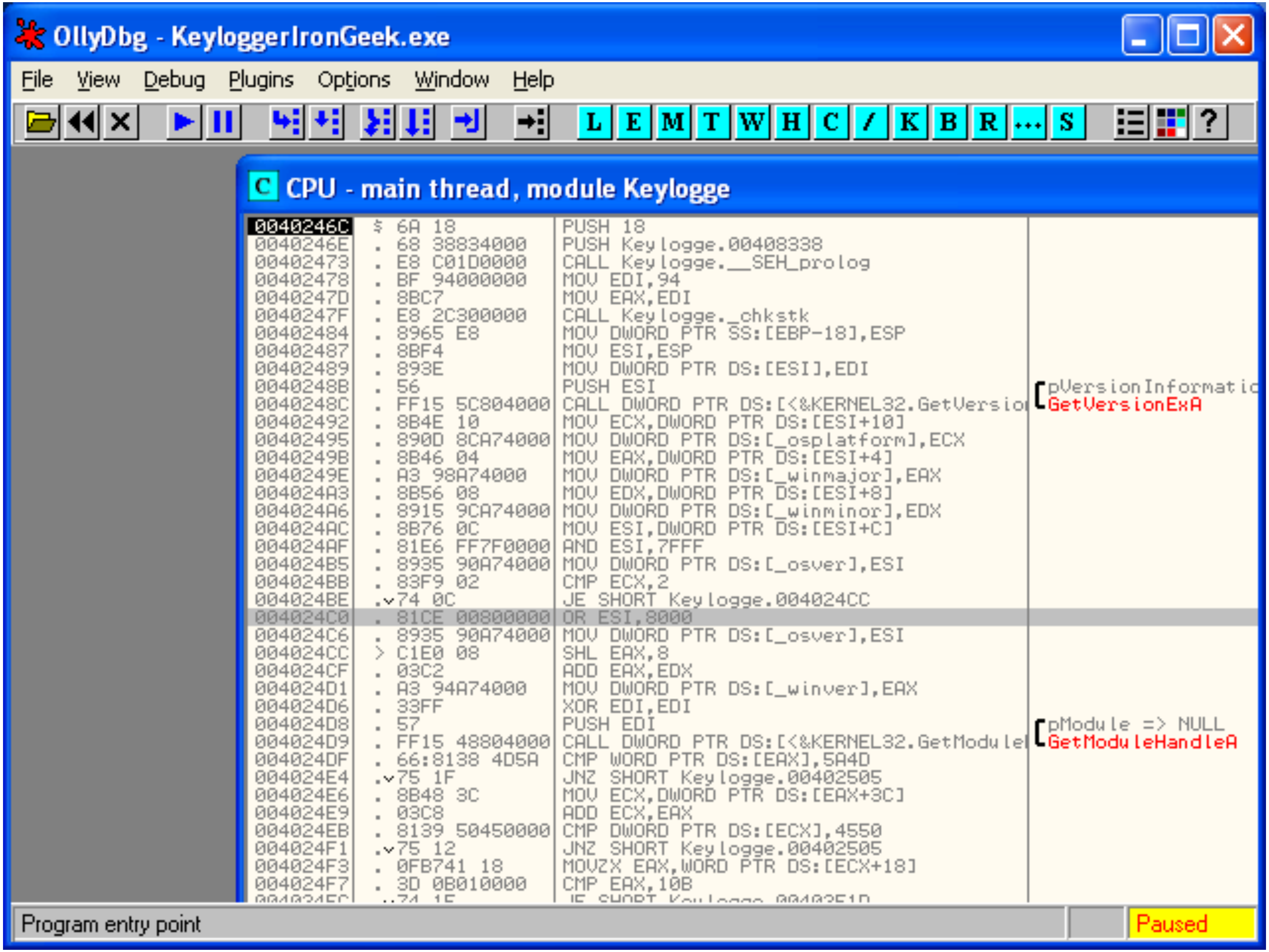
Name	A
F MailIt	00
F get_keys	00
F _main	00
C Sleep(x)	00
C AllocConsole()	00
C GetAsyncKeyState(x)	00
C ShowWindow(x,x)	00
C FindWindowA(x,x)	00
F closesocket(x)	00
F send(x,x,x,x)	00
F recv(x,x,x,x)	00
F connect(x,x,x)	00
F socket(x,x,x)	00
F htons(x)	00

Line 3 of 541

Address	Length	T...	String
"..." .rdata:0...	00000008	C	connect
"..." .rdata:0...	00000010	C	Connecting....\n
"..." .rdata:0...	0000000E	C	gethostbyname
"..." .rdata:0...	00000012	C	WSAStartup faile
"..." .rdata:0...	00000009	C	SMTP.log
"..." .rdata:0...	0000000D	C	smtp.scu.edu
"..." .rdata:0...	00000013	C	irong33k@gmail.
"..." .rdata:0...	0000000D	C	The Log Dude
"..." .rdata:0...	00000010	C	\r\n[CAPS LOCK
"..." .rdata:0...	00000009	C	\r\n['\"]\r\n
"..." .rdata:0...	0000000B	C	\r\n[ ]}]\r\n
"..." .rdata:0...	00000009	C	\r\n[\\|]\r\n
"..." .rdata:0...	0000000B	C	\r\n[[{]\r\n
"..." .rdata:0...	00000009	C	\r\n[`~]\r\n

```
e 'C:\Program Files\IDA\idc\onload.idc'...
ction 'OnLoad'...
ing the input file...
 to explore the input file right now.
ype' at 00408D10 is deleted...
ignature: Microsoft VisualC 2-7/net runtime
ype information...
gate_stkargs: function is already typed
ment information is propagated
utoanalysis is finished.
```

own | Disk: 15GB | 0000246C | 0040246C: mainCRTStartup


OllyDbg - KeyloggerIronGeek.exe
File
View
Debug
Plugins
Options
Window
Help
L
E
M
T
W
H
C
/
K
B
R
...
S
?
C
CPU - main thread, module Keylogge

```
0040246C  $ 6A 18          PUSH 18
0040246E  . 68 38834000    PUSH Keylogge.00408338
00402473  . E8 C01D0000    CALL Keylogge.__SEH_prolog
00402478  . BF 94000000    MOV EDI,94
0040247D  . 8BC7           MOV EAX,EDI
0040247F  . E8 2C300000    CALL Keylogge._chkstk
00402484  . 8965 E8        MOV DWORD PTR SS:[EBP-18],ESP
00402487  . 8BF4           MOV ESI,ESP
00402489  . 893E           MOV DWORD PTR DS:[ESI],EDI
0040248B  . 56             PUSH ESI                                   [pVersionInformatic
0040248C  . FF15 5C804000  CALL DWORD PTR DS:[<&KERNEL32.GetVersio    [GetVersionExA
00402492  . 8B4E 10        MOV ECX,DWORD PTR DS:[ESI+10]
00402495  . 890D 8CA74000  MOV DWORD PTR DS:[_osplatform],ECX
0040249B  . 8B46 04        MOV EAX,DWORD PTR DS:[ESI+4]
0040249E  . A3 98A74000    MOV DWORD PTR DS:[_winmajor],EAX
004024A3  . 8B56 08        MOV EDX,DWORD PTR DS:[ESI+8]
004024A6  . 8915 9CA74000  MOV DWORD PTR DS:[_winminor],EDX
004024AC  . 8B76 0C        MOV ESI,DWORD PTR DS:[ESI+C]
004024AF  . 81E6 FF7F0000  AND ESI,7FFF
004024B5  . 8935 90A74000  MOV DWORD PTR DS:[_osver],ESI
004024BB  . 83F9 02        CMP ECX,2
004024BE  .v74 0C          JE SHORT Keylogge.004024CC
004024C0  . 81CE 00800000  OR ESI,8000
004024C6  . 8935 90A74000  MOV DWORD PTR DS:[_osver],ESI
004024CC  > C1E0 08        SHL EAX,8
004024CF  . 03C2           ADD EAX,EDX
004024D1  . A3 94A74000    MOV DWORD PTR DS:[_winver],EAX
004024D6  . 33FF           XOR EDI,EDI
004024D8  . 57             PUSH EDI                                   [pModule => NULL
004024D9  . FF15 48804000  CALL DWORD PTR DS:[<&KERNEL32.GetModulel   [GetModuleHandleA
004024DF  . 66:8138 4D5A   CMP WORD PTR DS:[EAX],5A4D
004024E4  .v75 1F          JNZ SHORT Keylogge.00402505
004024E6  . 8B48 3C        MOV ECX,DWORD PTR DS:[EAX+3C]
004024E9  . 03C8           ADD ECX,EAX
004024EB  . 8139 50450000  CMP DWORD PTR DS:[ECX],4550
004024F1  .v75 12          JNZ SHORT Keylogge.00402505
004024F3  . 0FB741 18      MOVZX EAX,WORD PTR DS:[ECX+18]
004024F7  . 3D 0B010000    CMP EAX,10B
004024FC  .v74 1F          JE SHORT Keylogge.0040251D
```

Program entry point

Paused