

# **CSC 574**

# **Computer and Network Security**

## **Computer Forensics**

Alexandros Kapravelos  
kapravelos@ncsu.edu

(Derived from slides by Chris Kruegel)

# Computer Forensics

- Goal
  - explain the current state of a digital artifact
- Process
  - collect and analyze digital evidence
- Digital evidence
  - in principle, physical traces (e.g., magnetic fields on hard drives)
  - abstraction: bits -> characters -> file blocks -> files -> mail
  - each abstraction step must be documented (to hold in court)
    - but we focus here on the technical aspects
  - tons of digital traces everywhere
    - temporary files, logs, cache, backups, network packets, ...

# Forensics Process

- Seize evidence
- Preservation
  - ensure that evidence is not modified when analyzing
  - modifications can occur quickly (mount disk, boot computer)
- Recovery
  - obtain all data
  - hidden or deleted files
- Harvesting
  - obtain meta information about data
  - group by file type, access times, ...

# Forensics Process

- Reduction + Focus
  - filter irrelevant data
  - often, a huge problem due to data volume
  - hash database
    - NIST National Software Reference Library -- <http://www.nsrl.nist.gov/>
  - index data (like desktop search)
- Analysis and Reporting
  - scrutinize data to support hypothesis
  - write up (convincing) report

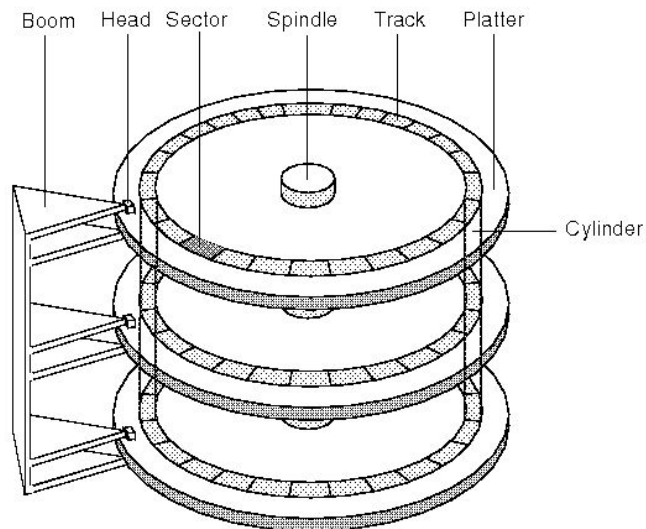
# Disk Analysis

- Hard disks
  - still the most significant source of digital evidence
- Analysis process
  - save (preserve) disk content
  - disk and partition analysis
  - file system analysis



# Disk Architecture

- Hard disk
  - several platters – disks (heads)
  - each platter has multiple tracks (start with 0)
  - each track has multiple sectors (start with 1)



# Disk Architecture

## Addressing sectors (blocks)

- CHS (cylinder, head, sector) triple
  - old disks use 10 bits for cylinder, 8 bits for head, 6 for sector
  - limits maximum disk size to ~ 8.4 GB
- Logical block address (LBA)
  - decouples logical and physical location
  - specifies 48 bit logical block numbers
  - allows controller to mask corrupt blocks

# Disk Architecture

## Disk Interfaces

between controller (motherboard) and disk

- ATA (AT Attachment)
  - 28 bit addresses (~128 GB maximum size)
  - 40 pin cables, 16 bit parallel transfer (single-ended signaling)
  - 2 devices (master and slave) can be attached to connection cable
  - ATA-3 introduced security features (passwords)
- Serial ATA (SATA)
  - 8 pin cables
  - higher data transfer (differential signaling)



# Disk Architecture

- Hidden protected area (HPA)
  - introduced with ATA-4
  - disk can be set to report to OS less blocks than actually available
  - remaining blocks can be used for data that is not formatted
    - utilities and diagnostic tools, but also malicious code or illegal material
- Device configuration overlay (DCO)
  - introduced with ATA-6
  - additional space (blocks) after HPA
  - used by manufacturers to shrink different disks to appear with exactly the same size

# Boot Process

- BIOS
  - firmware that holds starting code
  - performs system checks and loads MBR
- MBR (master boot record)
  - first block on hard disk (512 bytes)
  - structure
    - 446 bytes for code
    - 4 x 16 bytes for four partition table entries
    - 4 byte MBR signature (0xAA55)
  - chain loading of first block of bootable partition (OS loader)
- Interesting “return of the boot viruses”
  - Mebroot is a MBR virus that loads a stealth backdoor
  - patches Windows on-the-fly while it is loaded

# Analysis – Save Content

- What to save
  - typically at the level of disk blocks (less often, file system objects)
- How to access disk
  - talk to controller (ATA commands)
  - use BIOS routines (int 0x13)
  - use OS routines (`dd` for Linux)
- Caveats
  - make sure that no writes are performed (write blocker)
  - expect and handle corrupt blocks

# Analysis – Save Content

UltraBlock eSATA IDE / SATA (Read Only)

http://www.digitalintelligence.com/products/ultrablock\_esata\_ide-sata\_ro/

CS 290 DerStandard IJIS WWW '09 ICDCS '09 Usenix Sec '09 Danchev Honeyblog Google Security Blog Mark Russinovich Crypto Blog Freedom

**Digital Intelligence**  
mastering the science of digital forensics

HARDWARE SOFTWARE TRAINING SERVICES PURCHASE SUPPORT COMPANY INFO

SEARCH DIGITAL INTELLIGENCE

Go!

FORENSIC HARDWARE  
FORENSIC SOFTWARE  
FORENSIC TRAINING  
FORENSIC SERVICES

**HOLIDAY SCHEDULE**  
DI will be closed on the following dates:  
19-Jan-09 | Martin Luther King Day  
[SIGN UP ON THE DI MAILING LIST](#)

**ULTRABLOCK**



The **Read Only UltraBlock eSATA IDE-SATA** is used to acquire data from an IDE or SATA hard drive in a forensically sound write-protected environment. The eSATA Forensic Bridge supports four different host connection options for SATA and IDE device acquisitions:

- One eSATA
- Two FireWire800
- One FireWire400
- One USB 2.0/1.1

**UB eSATA IDE-SATA Read Only Kit \$429.00** [ORDER](#)

[larger image](#)

# Analysis – Save Content



## RoadMASter-3 Portable Forensic Lab



### Portable Forensic Evidence Seizure Preview and Analysis System

- The RoadMASter-3 Forensics System is designed as a high-speed Forensic Data Acquisition and Analysis tool.
- Ruggedised and built for the road, the unit provides for high-speed data seizures exceeding 3.5GB per minute.
- It supports today's common drive interfaces including P-ATA, S-ATA, SCSI and SAS drives, FireWire 1394A/B, USB1.0./2.0, Gigabit Ethernet and other solid state devices.
- While on location the Suspect's hard drive or the Evidence hard drive can be previewed under the Windows Operating System or analysed using third party data analysis software tools.
- Durability and performance makes this unit unique in the market place.

# Analysis – Partition Analysis

- MBR stores partition table
- Partition table
  - describes layout of a drive (disk)
  - has four slots
  - define start and end sector of different partitions
- Partition
  - in Windows, partition maps to a drive – such as c:\
  - in Unix, partitions are mapped into a single tree – starts at /
  - what about sectors that are not part of any partition?

# Analysis – Partition Analysis

- Extended partition
  - only four partitions possible (this is not enough)
  - solution – make one table entry pointer to an *extended partition*
- Extended partition
  - holds list of entries that point to more partitions
  - each entry stores size of partition and pointer to next entry
  - no limit (except disk space)

# Analysis – Partition Analysis

```
chris@segfault: hexdump -v ext-part-test-2.dd
```

```
.....
```

status (0x80 = boot, 0x00 = non-boot)

```
0000190 0000 0000 0000 0000 0000 0000 0000 0000 0000
00001a0 0000 0000 0000 0000 0000 0000 0000 0000
00001b0 0000 0000 0000 0000 fef4 8a8f 0000 0100
00001c0 0001 1f04 193f 003f 0000 cc81 0000 0000
00001d0 1a01 1f04 333f ccc0 0000 ccc0 0000 0000
00001e0 3401 1f04 4d3f 9980 0001 ccc0 0000 0000
00001f0 4e01 1f05 9a3f 6640 0002 5e60 0002 aa55
0000200 0000 0000 0000 0000 0000 0000 0000 0000
```

```
.....
```

partition type (0x04 = FAT 16)

# of sectors = 0x0000cc81 [52353]

LBA of first sector = 0x0000003f [63]



# Analysis – Partition Analysis

```
chris@segfault: mmls ext-part-test-2.dd
```

```
DOS Partition Table
```

```
Offset Sector: 0
```

```
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
00:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
01:	-----	0000000000	0000000062	0000000063	Unallocated
02:	00:00	0000000063	0000052415	0000052353	DOS FAT16 (0x04)
03:	00:01	0000052416	0000104831	0000052416	DOS FAT16 (0x04)
04:	00:02	0000104832	0000157247	0000052416	DOS FAT16 (0x04)
05:	Meta	0000157248	0000312479	0000155232	DOS Extended (0x05)
06:	Meta	0000157248	0000157248	0000000001	Extended Table (#1)
07:	-----	0000157248	0000157310	0000000063	Unallocated
.....					

# Analysis – File System

- File systems
  - come in many different flavors
  - in principle, OS independent
    - FAT can be read by Windows, Linux, ..
  - in some cases, certain OS has special behavior
    - Windows expects that FAT file system has correct magic values, Linux ignores that
- File system objects
  - layout information
  - file content
  - file meta-information (FAT entries, i-nodes)
    - name, size, last modification times, which blocks are used

# Analysis – File System

- Layout information
  - located in first block(s)
  - determine type of file system and location of other data structures (i-node blocks, FAT tables)
  - corruption is difficult to compensate
- Volume slack
  - unused blocks after file system

# Analysis – File System

```
chris@segfault: fsstat fat-img.dd
```

```
FILE SYSTEM INFORMATION
```

```
-----
```

```
File System Type: FAT16
```

```
OEM Name: mkdosfs
```

```
Volume ID: 0x3f441e25
```

```
Volume Label (Boot Sector):
```

```
Volume Label (Root Directory):
```

```
File System Type Label: FAT16
```

```
File System Layout (in sectors)
```

```
Total Range: 0 - 30719
```

```
* Reserved: 0 - 0
```

```
** Boot Sector: 0
```

```
* FAT 0: 1 - 119
```

```
* FAT 1: 120 - 238
```

```
* Data Area: 239 - 30719
```

```
** Root Directory: 239 - 270
```

```
** Cluster Area: 271 - 30719
```

# Analysis – File System

- File content
  - stored in blocks
  - allocation is file system dependent
  - blocks are often scattered over file system (fragmentation)
- Content analysis
  - check individual blocks or search for keywords/regular expressions
  - content might be split over block boundary
  - slack space (unused space in last block of file)
- File carver
  - programs that scan blocks for characteristic header/footer information used by applications (e.g., scalpel)

# Analysis – File System

- File metadata
  - useful to narrow down search
    - e.g., all files that were created after certain time
  - can be manipulated
  - metadata space can also be used to hide data

# Analysis – File System

- File deletion
  - different file systems handle deletion differently
  - typically, only metadata is deleted
  - as a result, data content remains on disk
- Undelete
  - in FAT
    - only first character of directory entry is deleted
    - FAT table entries are freed
    - for non-fragmented files, undelete is quite easy
  - for other systems, often more difficult

# Analysis – File System

Securely destroying / deleting data is difficult

Department of Defense Manual 5220.22 M

1. Degauss with a Type I degausser (degaussing exposes the drive to an electromagnetic field)
2. Degauss with a Type II degausser
3. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAIN TOP SECRET INFORMATION.
4. Destroy –Disintegrate, incinerate, pulverize, shred or smelt.



# Analysis – File System

May 31, 2005 3:02 PM PDT

## Dumped hard drives tell all

Posted by Joris Evers



Font size



Print



E-mail



Share



Post a comment

## Sensitive corporate data just \$10 on eBay

OUT-LAW News, 09/06/2004

**Laptops and hard disks containing sensitive corporate data are readily available at auction sites. Researchers paid \$10 for a hard disk from eBay which came with access codes to the secure intranet of one of Europe's largest financial services groups.**

It was the first of 100 disks and laptops purchased as spare and used parts from internet auction sites as part of a study into the accessibility of information from lost laptops and hard disks.

In the study by security specialists Pointsec Mobile Technologies, seven out of ten of the disks, all of which were supposedly "wiped-clean" or "re-formatted," contained readable information.

one state bank system, the computer system, the computer system, the United States Veterans Administration Medical Center in Indianapolis retired 139 computers. Some of these sys-

tem computer systems from a local computer store. The computers, most of which were three to five years old,

PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/05/17.00 © 2005 IEEE ■ IEEE SECURITY & PRIVACY

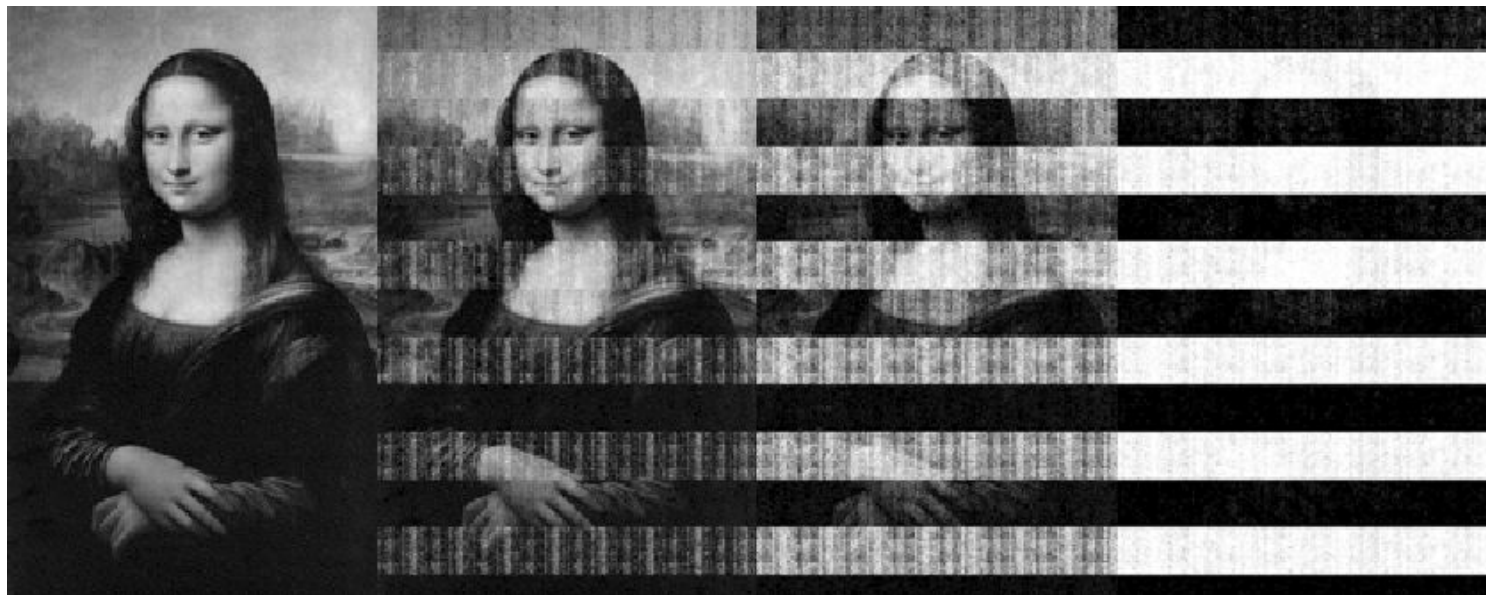
17

# Live System Analysis

- When system is running, additional information can be collected
  - active connections
  - active processes
  - loaded kernel modules
  - open files
  - clear text passwords (that are only resident in memory)
- Problems
  - analysis modifies state of system
  - rootkits (or other modifications) can tamper with results
- Memory dumps
  - take snapshot of memory of running system for later examination
  - can be done by software (/dev/kmem) or hardware extensions

# Live System Analysis

- Physical (volatile) memory is also more persistent than one thinks
- Cold boot attacks
  - Lest We Remember: Cold Boot Attacks on Encryption Keys  
Haldermann et al. (Usenix Security Symposium, 2008)
  - RAM taken out of computer and scanned for sensitive content



# OS Papers

seL4: Formal Verification of an OS Kernel

Klein et al.

ACM Symposium on Operating Systems Principles (SOSP), 2009

Make Least Privilege a Right (Not a Privilege)

Krohn et al.

HotOS 2005

EROS: A Fast Capability System

J. Shapiro et al.

Symposium on Operating Systems Principles (SOSP), 1999



A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

- Dro
- 68m
- http



**Dropbox:** In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

**Compromised data:** Email addresses, Passwords



**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords



**Malwarebytes:** In November 2014, the Malwarebytes forum was hacked and 111k member records were exposed. The IP.Board forum included email and IP addresses, birth dates and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

**Compromised data:** Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity



**MySpace:** In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

**Compromised data:** Email addresses, Passwords, Usernames



**tumblr:** In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

**Compromised data:** Email addresses, Passwords