Digital Forensics 2.0

SBA Research &
Vienna University of Technology

Edgar R. Weippl

Overview

- Definition
- Digital Evidence
- How is a forensic investigation done today?
- What are future challenges?

Definition

- Forensic science is generally defined as the application of science to the law.
- "Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data"
- Source: NIST SP 800-86

Digital Evidence

- Growing importance since life becomes digital.
- Movies, series: CSI, ...
- Research papers: iPhone & Android Forensics, Cloud Forensics, Social Network Forensics, …
- Becomes important for companies, budget increases

Digital Evidence

- Corporate Governance creates new responsibilities
  - Some person / department has to address information security.
  - Incident response is part of information security management
  - Management want explanations about what happened
- ISMS requires traceability of incidents

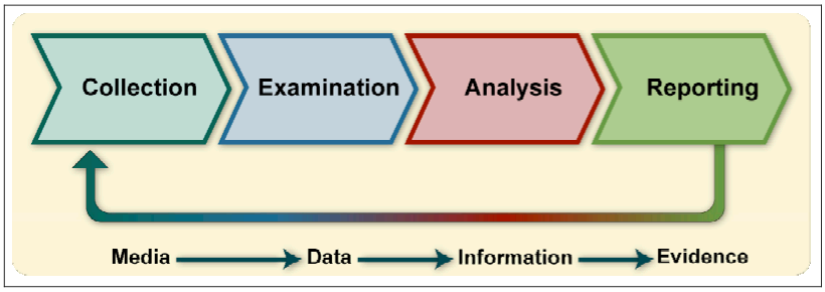
Digital Evidence

- White-collar crime often uses computers / networks
- Companies realize the potential losses such as
  - Media companies (music, movies, ...)
  - Software license
  - Employees using company equiment used privately

Increased Perception

- Sabu / Lulzsec, Anonymous, …
- „Cyber Warriors“, such as United States Cyber Command in .us, …
- „Cyber Defense“
  - 1600 in Austria, LKA / BKA
  - CCC in Germany
  - Cooperative Cyber Defense Centre of Excellence (CCDCoE) by NATO in Tallinn …)

Guide to Integration Forensic Techniques into Incident Response (NIST 800-86)



Data Collection

- Identifying possible sources of data
- Acquiring the data
  - Develop a plan to acquire the data
    - Likely Value
    - Volatility
    - Amount of Effort Required
  - Acquire the data
  - Verify the integrity of the data

Reporting

- Alternative Explanations
- Audience Consideration
- Actionable Information

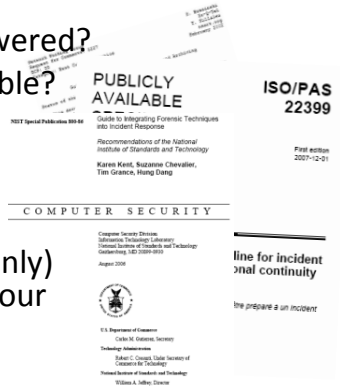
Recommendations

- Organizations should perform forensics using a consistent process
- Analysts should be aware of the range of possible data sources
- Organizations should be proactive in collecting useful data
- Analysts should perform data collection using a standard process
- Analysts should use a methodical approach to studying the data
- Analysts should review their processes and practices

Different Methods

Methods depend on the task at hand

- What needs to be examined?
  - Which question should be answered?
  - Which artifacts are (still) available?
- Which tools?
  - Depends on data
- Which methods?
  - Is this a court case or do you (only) need to know where to focus your attention?

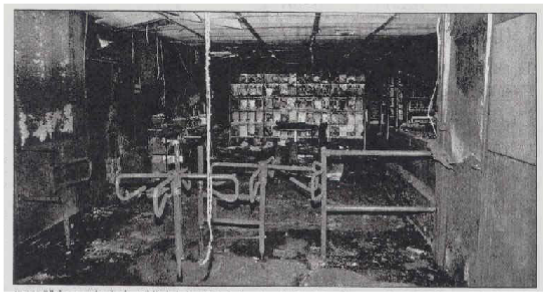


Example

Brandstiftung: WU- Gebäude muss schließen
Der Standard, 15.12.2005, Seite 1

Brandstiftung: WU-Gebäude muss schließen

Wien – Brandstiftung ist nach ersten Ermittlungen der Polizei die Ursache für ein Feuer in der Wiener Wirtschaftsuniversität (WU), das den Uni-Betrieb in Turbulenzen stürzt. In der Nacht von Dienstag auf Mittwoch wurde an vier Stellen des Gebäudes in Wien-Alsergrund Feuer gelegt. Vor allem die Bibliothek ist dadurch schwer beschädigt worden, 20.000 Bücher wurden zerstört. Nach Einschätzung der Uni-Leitung bleiben die Bibliothek und das Hauptgebäude, die von rund 21.000 Studierenden benutzt werden, zumindest bis Ende der Woche geschlossen. (red) S. 13



Methods

Timeline Analysis

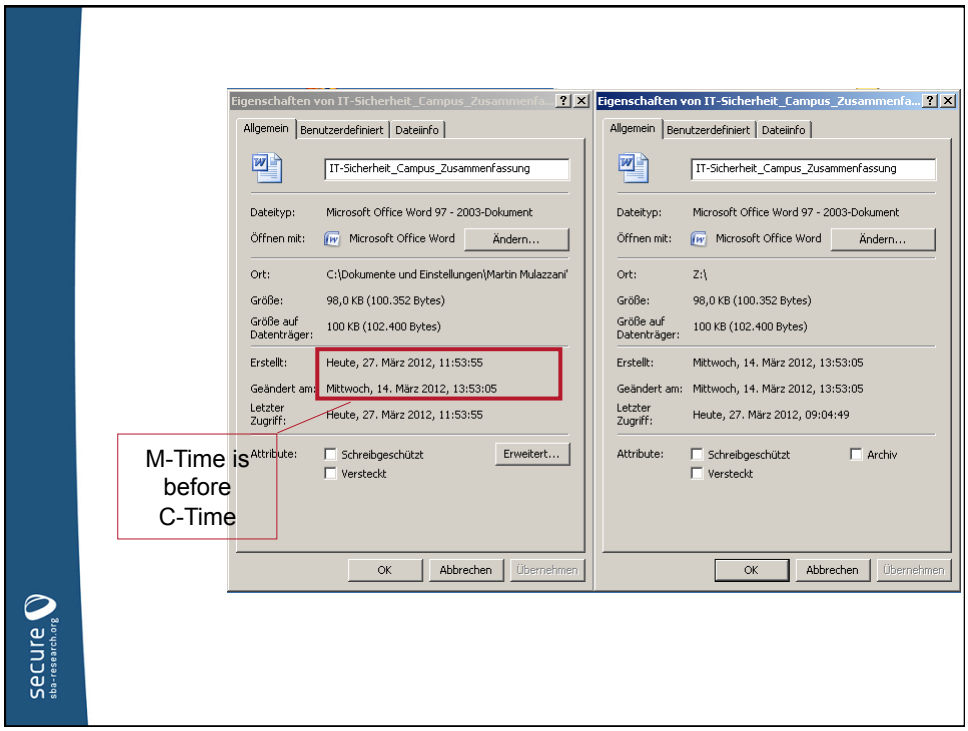
- Reconstruct series of events
- Data sources
  - Meta data on file system
  - Can sometime be recovered for deleted data
  - MAC time stamp

Time Stamps

- Last access to a file
  - M odified (last write)
  - A ccessed (write/read also modified for read-only)
  - C reated / changed (modification of attributes)
- Copy / Move may behave differently
- Unix / Windows behave differently
- Users, malware, programs can modify time stamp (e.g. touch, Total Commander)

Time Stamps

- Strange behavior when copying/moving files in NTFS
- Copy: M-time is before C-time
- Identification of source and target possible
- However: A-Time is not updated on Vista and NTFS by default (NtfsDisableLastAccessUpdate = 1)
- Linux mount flag noatime



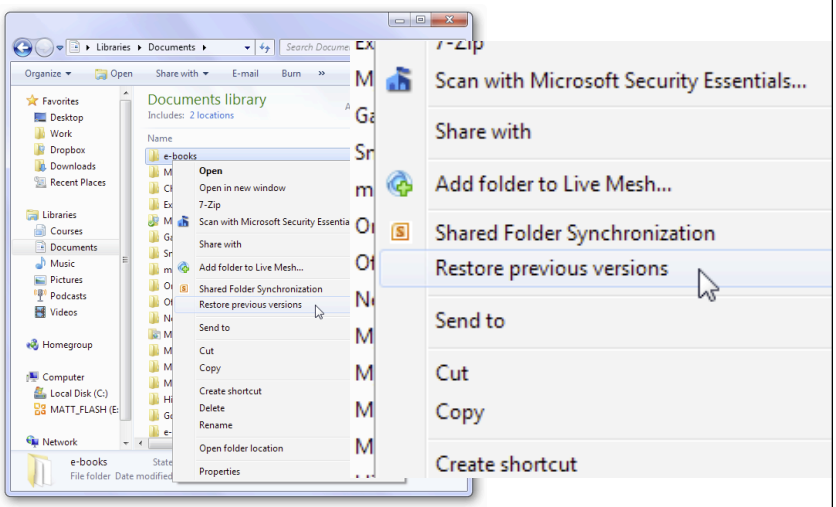
FAT and NTFS

ACTION	LAST MODIFIED DATE-TIME	LAST ACCESSED DATE-TIME	CREATED DATE-TIME
File moved within a volume	**Unchanged**	**Unchanged**	**Unchanged**
File moved across volumes	**Unchanged**	**Updated**	**Updated**
File copied (destination file)	**Unchanged**	**Updated**	**Updated**

Timeline Analysis

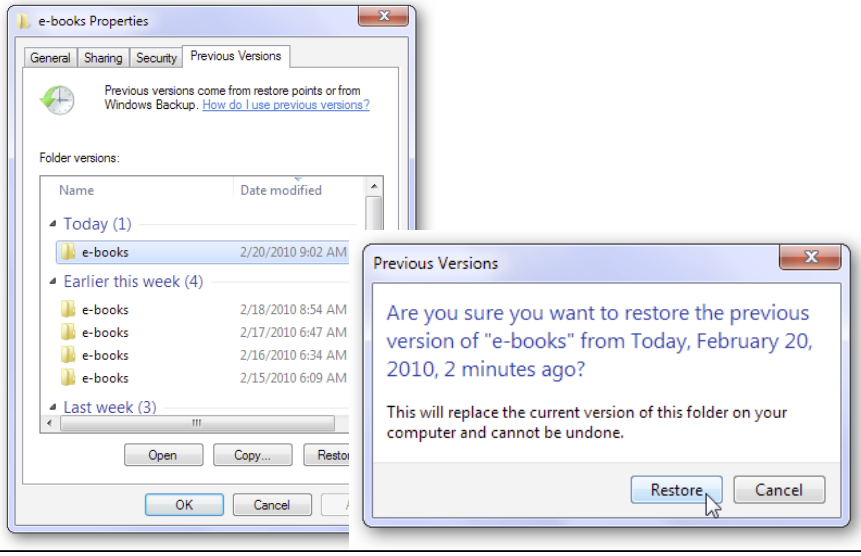
- For each file it is possible to reconstruct what happened
  - Dropbox pack rat feature
  - When was file written, modified, change history
  - Was the file modified after accessing a Web site

Volume Snapshot Service

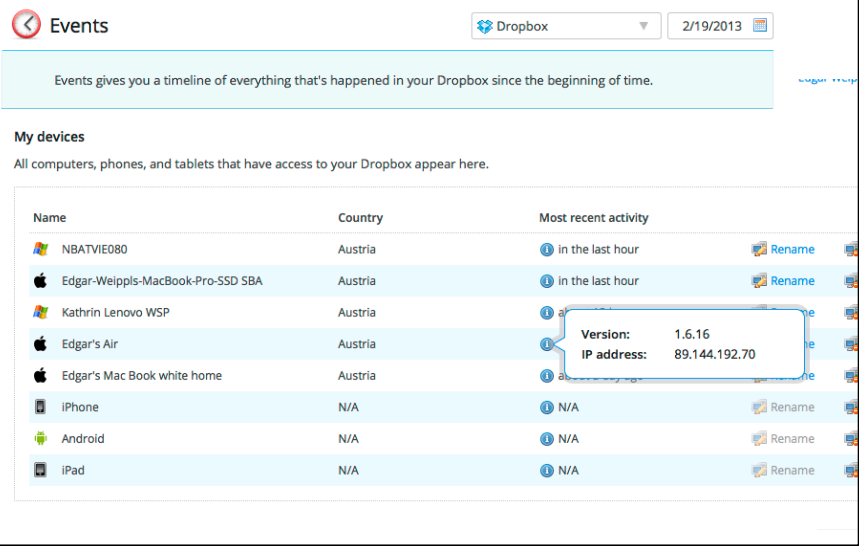


- Source http://www.howtogeek.com/howto/11130/restore-previous-versions-of-files-in-every-edition-of-windows-7/

Volume Snapshot Service



Dropbox



Internet Explorer History

- **Http-Auth:** %APPDATA %\Microsoft \Credentials, in encrypted files
- **Form-based:** HKEY_CURRENT \Software\Micro \Internet Explor \IntelliForms\St encrypted with t
  - http://securityxploded.com/iepassworddecryptor.php

Network Traffic

- Rootkits can hide processes, files
- Do not trust the operating system

- Data traffic is difficult to hide
- SSL – man in the middle
- TCPDump (IP address, ports, content)

Example

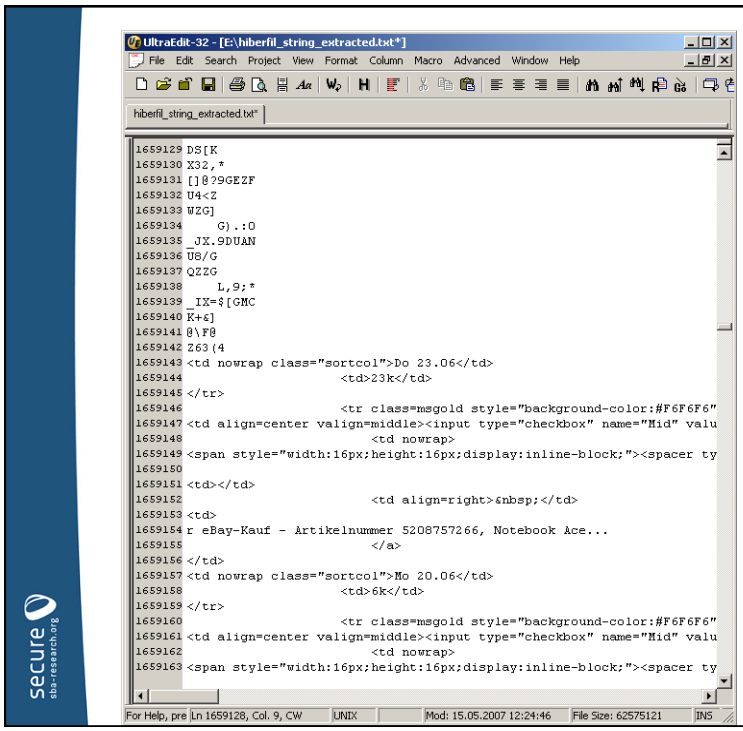
- For our example:
  - No network traffic available
  - Only two laptop recovered

Keyword Search

- Search in
  - Files
  - Empty space
  - Swap files, swap partitions
  - RAM

For key words; use word lists…

- E.g. strings RAMDump.bin | grep DVDRip



Search for „Kanister“ (fuel can)

Example

- Arson?
  - Bid to buy a fuel can
- No proof but indicates that further investigation makes sense
- Investigation is usually time-bounded.

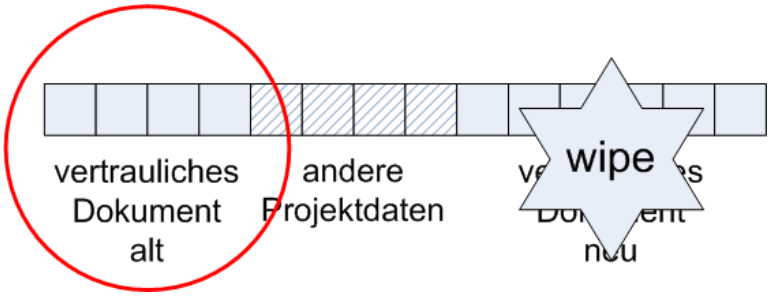
Reconstruction of Data

Deleted files

- Trivial
  - Only reference to file is deleted
  - Files are marked as deleted
  - Files can be recovered with high probability
  - Also applies to cameras, smartphones, …
- Advanced
  - You create a document, other processes in the background do other stuff, you add data to your document.
  - What happens if you use a secure delete on the file?

Copy-On-Write File System (e.g. BTRFS) or some SSDs

- Document can be recovered



File Carving

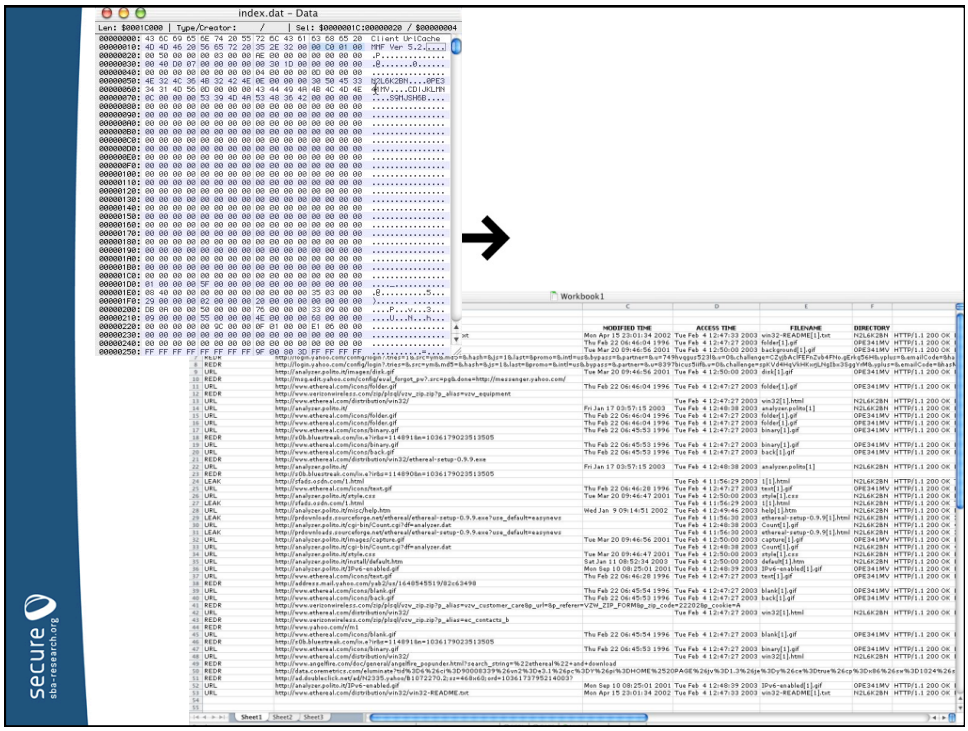
- Search for characteristic signatures of files
  - JPEG files start with 0xffd8 and end with 0xffd9
- Tools such as Foremost look for these signatures

Example

- Let's get back to our example:
  - A file could be found (as deleted)
  - No new additional evidence could be found

Internet Browser History

- Tool Pasco
  - Cached Files are stored in index.dat (Internet Explorer)
  - Pasco can extract these and display results
- Details: Keith J. Jones, 2003, „Forensic Analysis of Internet Explorer Activity Files"



More Sources

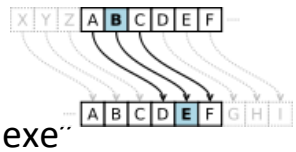
- Look at other commonly used programs
  - E-Mail (Outlook, mbox) with tools such as scanpst
- Google Desktop Search
  - Benjamin Turnbull et.al. , “Google desktop as a source of digital evidence”, International Journal of Digital Evidence, Fall 2006, Volume 5, Issue 1

Windows Desktop Search

- Installed by default since Vista
- File Windows.edb
- Tools: esedbtools, EseDbViewer
- File location: %Profiles%/All Users/Application Data/Microsoft/Search/Data/Applications/ Windows/
- May contain entire files or parts such as e-mails, documents,
- Paper by Joachim Metz, „Forensic analysis of the Windows Search database"

Last Commands and Applications Started

- Last commands and applications executed by a user (eg. Windows User Assist Key)
- "HKEY_USER\<sid>\Software\Microsoft \Windows\CurrentVersion\Explorer\UserAssist \{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count"
- "Encrypted" with ROT13 cipher: "T:\rapnfr3.rkr " -> "g:\encase3.exe"
  - set "NoEncrypt=1" to stop encrypting and "NoLog=1" to stop logging altogether



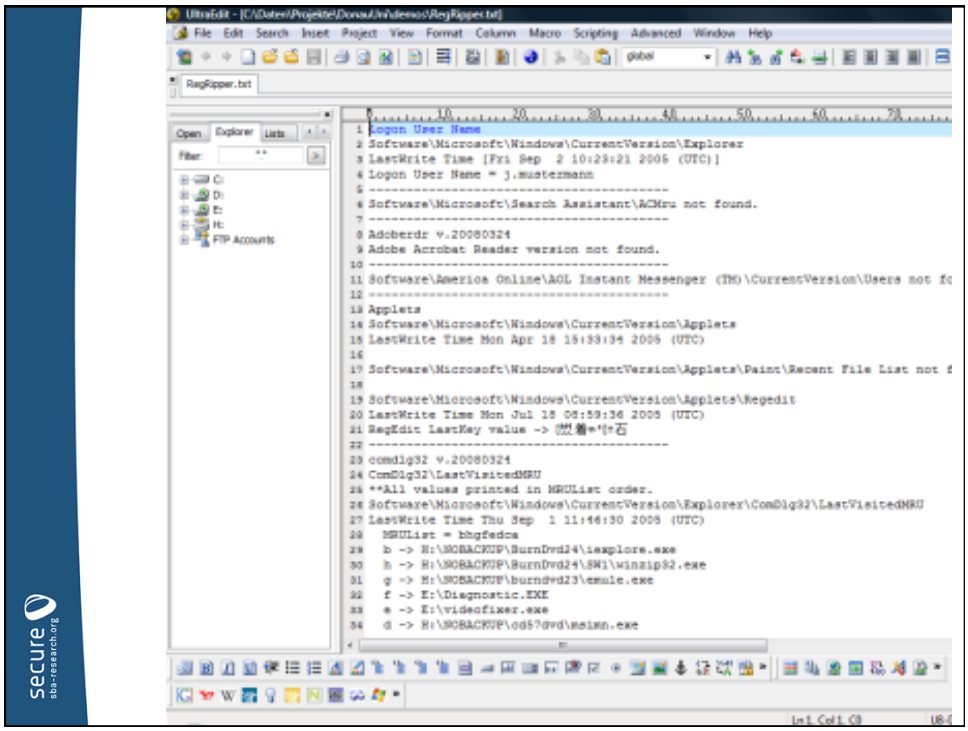
Windows User Assist Key Analysis (Windows 7)

Source: http://blog.didierstevens.com/2009/01/18/quickpost-windows-7-beta-rot13-replaced-with-vigenere-great-joke/

- "Weak ROT13 crypto has been replaced with "stronger" Vigenère crypto!"
- "The Vigenère key I found through some basic cryptanalysis is WHQNKTEZYFSLMRGXADUJOPIVC."
- "To the Microsoft developer who designed this: great joke! You really made me laugh. Seriously."

Registry Ripper (RegRipper)

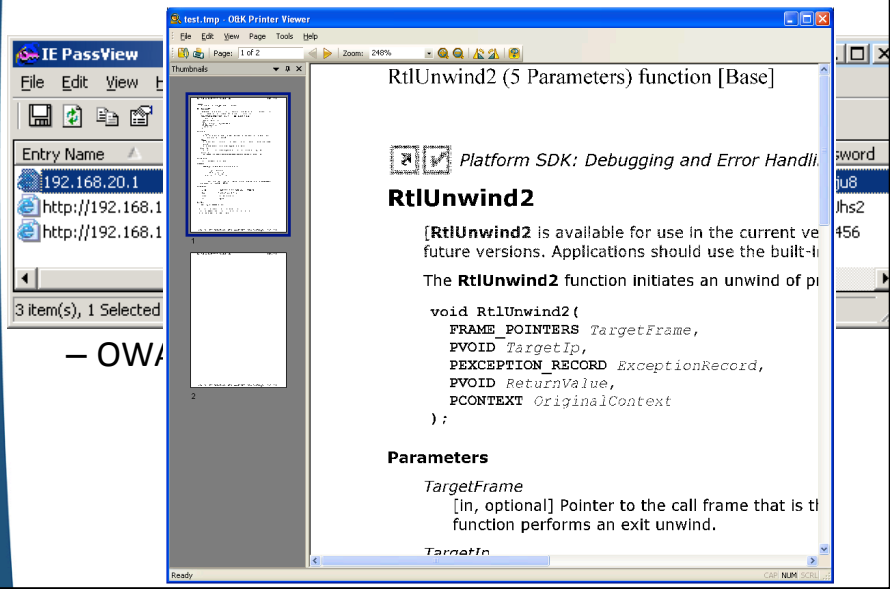
- Files played in media player
  - "HKEY_USERS\<sid>\Software\Microsoft\MediaPlayer\Player\RecentURLList"
- ZIP Files opened/saved with "common dialog"
  - "HKEY_USER\<sid>\Software\Microsoft\Windows\CurrentVersion\Explore\ComDlg32\OpenSaveMRU\zip"
- "<sid>" = Security Identifier of user
- RegRipper: http://regripper.wordpress.com



More traces…

- Prefetch files (Win XP)
- Deleted images (with foremost)
- IE password / account / autocomplete recovery
  - IE Passview
  - OWADE
- Spooler files
  - Contains pages printed www.prnwatch.com

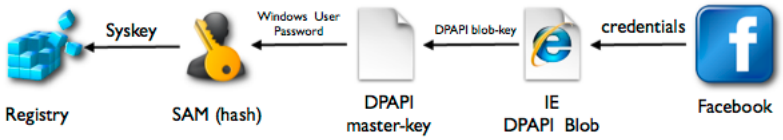
More traces…



– OWA

OWADE

Source: http://www.slideshare.net/jmichel.p/owade



Getting Facebook credentials require to bypass 4 layers of encryption

OWADE

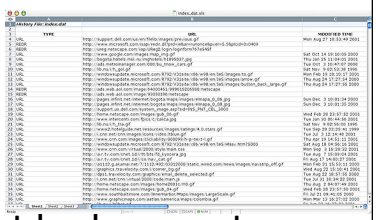
Source: http://www.slideshare.net/jmichel.p/owade

Geolocation / WLAN

- Info stored for each access point
  - Mac address (BSSID)
  - Key (encrypted)
  - Last time of access
- Wifi data are stored in
  - Registry (XP)
  - XML file and Registry (Vista/7)

Source: http://www.slideshare.net/jmichel.p/owade

Let's get back to our example



- Analyze hard drive IE history (Pasco, index.dat)
- We could show that suspect had access to Web mail account of sender.
- Username/PW Kombination for Web mail account were found and still valid.

secure sba-research.org

derStandard.at | **Panorama** | **Wien**

25. Juli 2007
20:22 MESZ

Nachlese: Bibliothek vom Brand am stärksten betroffen - eine Ansichtssache

Sechs Jahre Haft für WU-Brandstifter

Für die Richterin stand fest: Den "großen Unbekannten" Angeklagte hat den verheerenden Brand gelegt

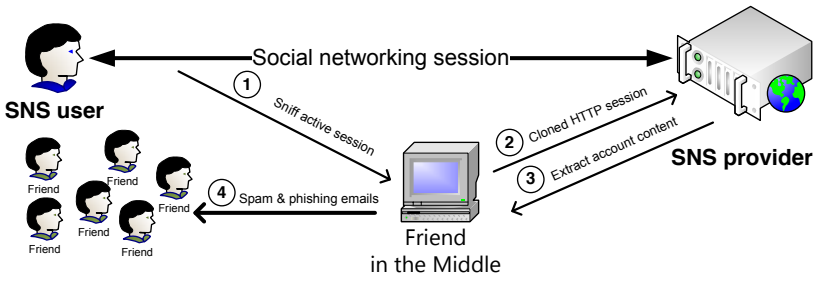
Wien - Natürlich muss sich der Prozessbeobachter die F niemand für Rudolf S. ein psychiatrisches Gutachten ge der Mann, der am Mittwoch wegen der Brandstiftung in Wirtschaftsuniversität (nicht rechtskräftig) zu sechs Jah worden ist, hat während der vier Prozesstage mitunter

Anonyme Mails

Dass auf seinem Laptop Texte gefunden worden sind, die große Ähnlichkeiten mit zwei anonymen Bekennermails an die Kriminalpolizei haben, wiegt schon schwerer. Vor allem, weil darin Details standen, die öffentlich nicht bekannt waren. Und dass der Sachverständige auch noch die Zugangsdaten für die E-mail-Adresse, von der die beiden Botschaften verschickt worden sind, auf dem Laptop entdeckt hat, machte die Verurteilung praktisch fix.

http://derstandard.at/druck/?id=2972033

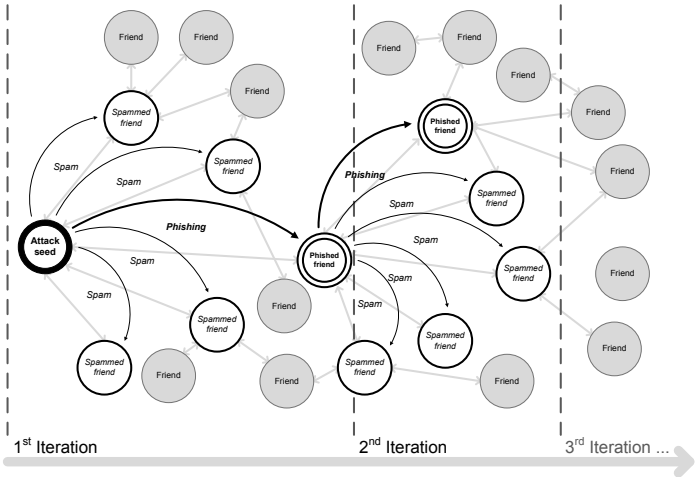
Friend-in-the-middle (FITM) attacks



- Hijack social networking sessions
- Attack surface: unencrypted WLAN traffic, LAN, router etc.
- User impersonation

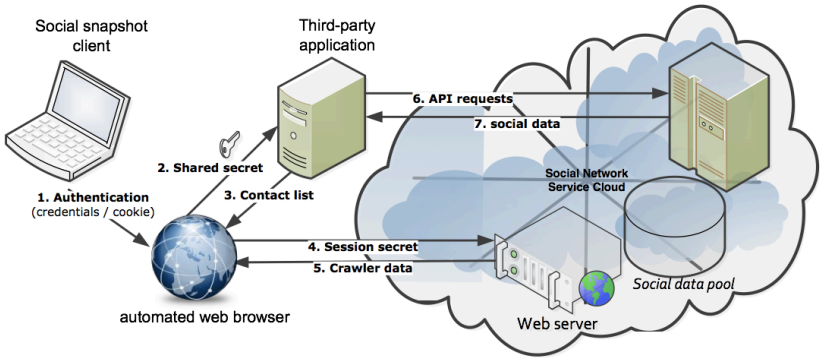
Markus Huber, Martin Mulazzani, Manuel Leithner, Sebastian Schrittwieser, Gilbert Wondracek, and Edgar R. Weippl. **Social snapshots**: Digital forensics for online social networks. In Annual Computer Security Applications Conference (ACSAC), 12 2011.

Attack scenario



Fast Access to Data:

Collection of digital evidence through our social snapshot application

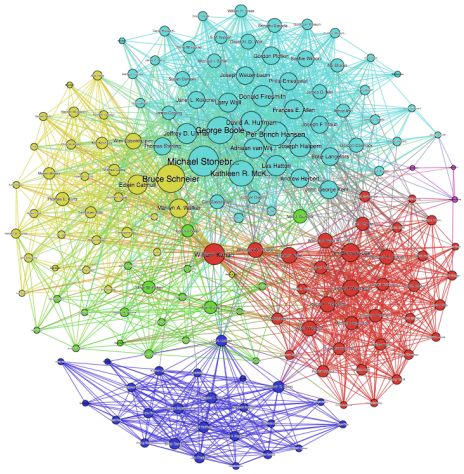


Access to Data

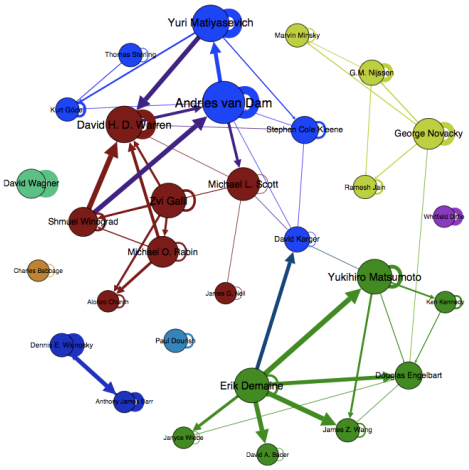
Element	Download	social snapshot
Contact details	–	✓Crawler
News feed	–	✓Graph API
Checkins	–	✓Graph API
Photo Tags	–	✓Graph API
Video Tags	–	✓Graph API
Friends	name only[a]	✓Graph API
Likes	name only[a]	✓Graph API
Movies	name only[a]	✓Graph API
Music	name only[a]	✓Graph API
Books	name only[a]	✓Graph API
Groups	name only[a]	✓Graph API
Profile feed (Wall)	limited[b]	✓Graph API
Photo Albums	limited[b]	✓Graph API
Video Uploads	limited[b]	✓Graph API
Messages	limited[b]	✓Graph API

[a] No additional information available.
[b] Missing meta-information such as UIDs.

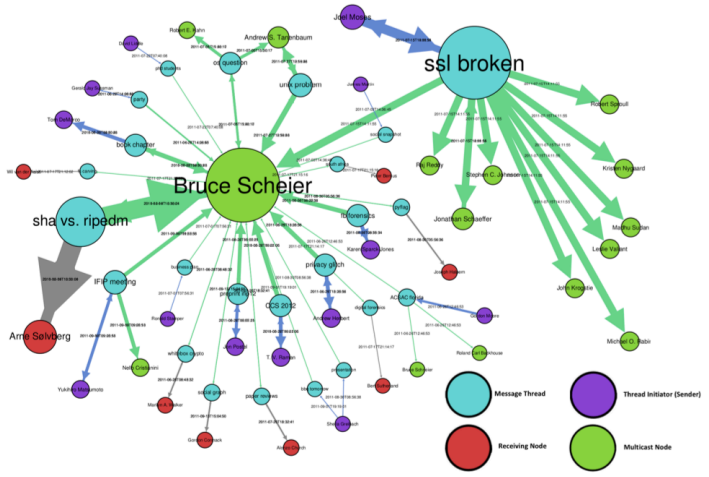
Anonymized Social Interconnection Graph



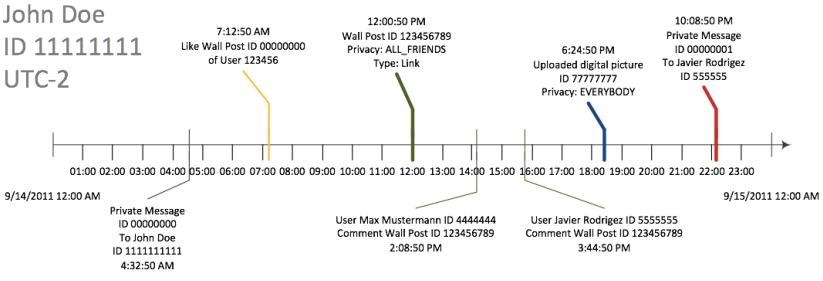
Anonymized Social Interaction Graph using Picture Tags



Social interaction graph using direct messages



Example timeline



Order of Volatility

- „Order of Volatility“ – RFC 3227:
  - registers, cache
  - routing table, arp cache, process table, kernel statistics,
  - memory
  - temporary file systems
  - disk
  - remote logging and monitoring data that is relevant to the system in question
  - physical conguration, network topology
  - archival media
- http://www.ietf.org/rfc/rfc3227.txt

Order of Volatility

- „Order of Volatility” - NIST 800-86
  - Network connections
  - Login sessions
  - Contents of memory
  - Running processes
  - Open files
  - Network configuration
  - Operating system time
- http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Challenges with Acquisition

- dead man's control: shutdown, reboot
- Running rootkit
- OS logging – modify settings or not?
- Computer runs but locked
- Shutdown or pull the plug?
- Key remapping
- Superuser or user-level access?
- Pre-incident installation
- …

Challenges with Acquisition

- Documentation!
  - In which state was the computer encountered?
  - What did you do?
  - Which software did you use? (exact versions!)
  - Which data did you copy to which location?
  - Hash values

Challenges with Acquisition

- Acquisition – Hardware vs. Software:
  - Software cheap but modifies state
  - Software can be tricked (kernel level Rootkit)
  - Hardware access requires additional hardware (DMA), such as Firewire, PCI, or PCMCIA
  - Hardware OS independent
  - Hardware can also be tricked (Rutkowska, BH 2007)
- There is no perfect answer!

Challenges with Acquisition

- Acquisition of virtual machines:
  - Suspend VMWare, copy *.vmem* file
- Windows Hibernation files
  - hiberfil.sys: switch to Hibernation Mode, copy file from hard disk
  - Not possible with Windows XP > 4 GB RAM

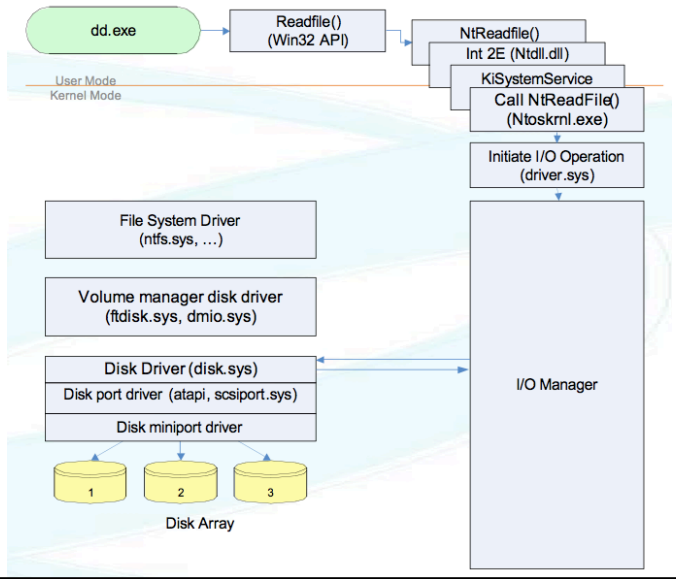
RAM Acquisition

- Image File Formats:
  - Raw – mit *dd* 1:1 image
  - Dumpfiles *.dmp* – CPU States information, required for Microsoft Tools
- Tools for Acquisition:
  - Kntdd – physical memory evidence from Microsoft Windows (XP, Win7, Win8)
  - Windd – disk dump
  - (Almost) all vendors (Encase, FTK, …) have free utilities or Live CDs such as *FTK Imager*

RAM Acquisition

- Example for Windows – **NOT** good:
  - psexec \\target –u Administrator –p password dd.exe if=\\.\PhysicalDrive0 of=\\mymachine\share $\target.drive0.dd bs=8k conv=noerroe
- \\.\PhysicalDriveX are hard disks
- \\.\PhysicalMemory is RAM
- Better use FTK Imager
- Source *www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Bilby-up.pdf (*Low Down and Dirty: Anti-forensic Rootkits - Black Hat)

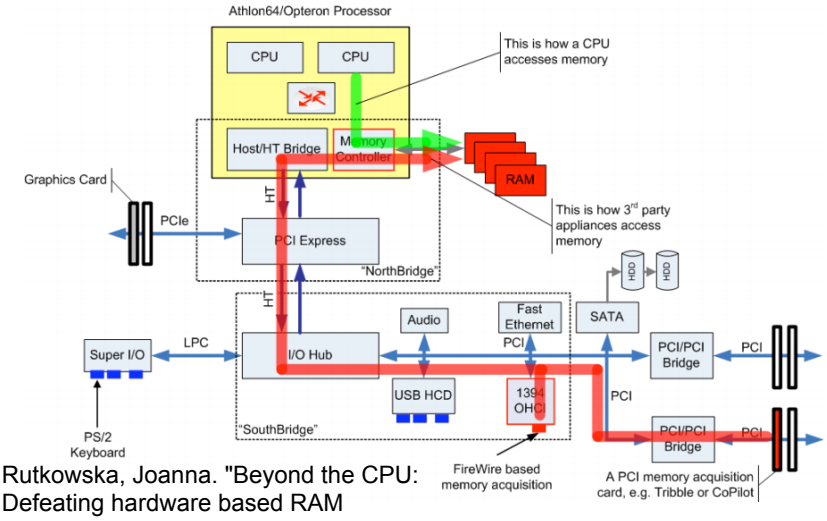
RAM Acquisition



RAM Acquisition

- Bilby‘s DDefy, Blackhat JP 2006
  - Protects against acquisition software
  - Modifies Page Fault Handler
  - Marks pages as „not present“
- Rutkowska DMA Redirection, Blackhat 2007
  - Protects against acquisition hardware
  - Reconfigures Northbridge
  - CPU & DMA see different content at same address

DMA – Rutkowska 2007



Rutkowska, Joanna. "Beyond the CPU: Defeating hardware based RAM acquisition." Black Hat DC (2007).

Cold Boot Attack

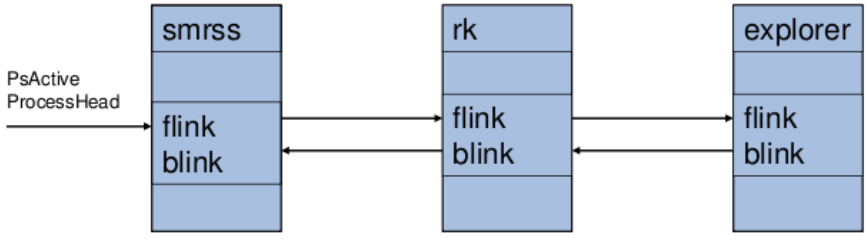
- *Lest We Remember: Cold Boot Attacks on Encryption Keys*, USENIX Security Symposium 2008
- Access RAM
  - Originally designed to capture crypto keys
  - Also useful for forensics (Screen locked, no USB, CD drive, investigator cannot start any external application)
  - Requires physical access

Windows RAM

- List of processes:
  - In Windows: all processes are in double chained list
  - Processes are objects
  - PsActiveProcessHead points to first element
  - Iterate shows all processes
  - Problem: root kits can modify the chain and make themselves invisible
  - What to do: scan entire memory; slow, specific of OS, difficult to do

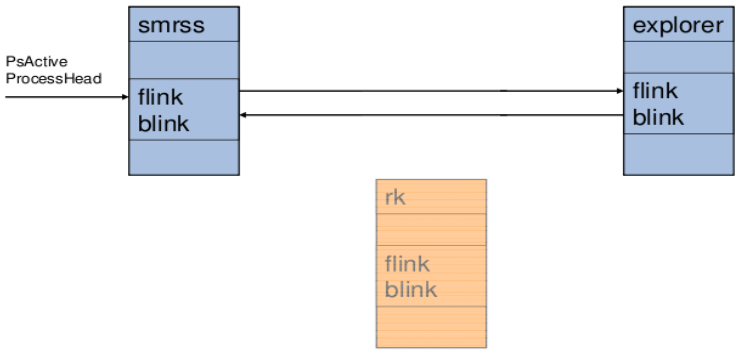
Windows RAM

Enumeration of processes



Windows RAM

- Antiforensics: DKOM manipulation (Direct Kernel Object Manipulation)



Windows RAM

- Timeline can be generated after RAM has been saved
  - Threads & processes: created, terminated
  - Registry: last modification
  - Sockets: time of creation
  - Objects: almost everything (in Windows)!:
    - File objects, Symlink Objects, Mutex, …

Windows RAM

- Tools you can use:
  - FTK 3
  - EnCase
  - …
- Open Source:
  - *Volatility!*

Windows RAM

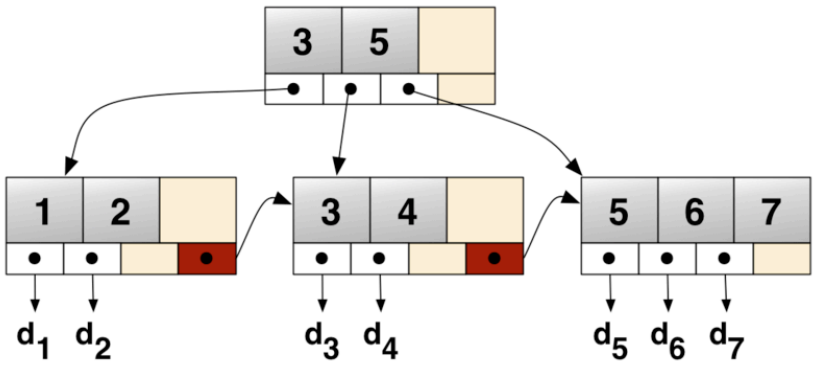
- *Volatility*:
  - For Windows XP, Vista, 7, Server 2003 & 2008
  - www.volatilesystems.com/default/volatility
  - Available for EnCase
- *ptfinder*:
  - Original by Andreas Schuster
  - Development was continued for 2008 Server & Windows 7

Windows RAM

- Volatility – selected commands:
  - strt: *„python vol.py commands“* or. *„python volatility commands“*
  - Convert images : *imagecopy*
  - Threads: *thrdscan*
  - Processes: *pslist, psscan, pstree, procexecdump, procmemdump*
  - Drivers: *driverscan*
  - Files: *filescan*
  - Sockets: *sockets, sockscan*
  - Connections: *connections, connscan, netscan*

RESEARCH IDEAS

B+ trees



Data Provenance Challenges

- Confidentiality
  - Cloud storage (e.g.Dropbox)
  - Authentication (e.g. WhatsApp)
  - Open data vs. unintended data leaks
- Availability
  - Dependability on infrastructure
  - Complex and hidden dependability
- Integrity
  - incomplete data,
  - entry errors,
  - processing,
  - sensors,
  - social media,
  - latency of information,
  - deception,
  - modeling approximations

And even more challenges
Data Provenance Challenges

- Privacy
  - Combining different data sources (e.g. reading habits, diets)
  - Ambiguity of data and incorrect conclusions
- Security
  - Data and provenance do not share the same access policy
  - Detecting fake or fabricated records
- Object removal
  - How to preserve ancestral relation?
- Minimization
  - Provenance can get much bigger than actual data
  - Storing provenance costs
  - Even when minimized, has to be updated, queried, used

Questions?

eweippl@sba-research.org