Forensic Analysis

The Treachery of Images

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

February 27, 2009

Disclaimer

Ceci n'est pas une pipe.
Magritte

Rene Magritte "La Trahison des Images" ("The Treachery of Images") (1928)

Gangster Story

- The Italian gangster and forensic analysis...

Gangster Story

- Moral of the story : "learning forensic analysis is useful even for Italian gangster".

Forensic Analysis - Theory

- Broad definition of (computer) forensic analysis : *"Forensic analysis involves the preservation, identification, extraction, documentation and interpretation of computer data"*
- *To reach those goals, the forensic specialists follow clear and well-defined methodologies. Flexibility is highly required when encountering the unusual.*

Forensic Analysis - Theory - Methodology

- Acquire the evidence without altering or modifying the original source.
- Authenticate that you gathered the evidence in a proper way.
- Analyze the non-original collected data without modifying it.

Forensic Analysis - Theory - Methodology

- Act always in ways that you can easily explaing to a court.
- Think twice before doing any action on the collected data.
- Take notes of everything not only the action taken but also any discoveries.

Forensic Analysis - Theory - The Order of Volatility (OOV)

The expected life of data :

Type of Data	Life Span
Registers or cache	Nanoseconds
Main Memory	Ten Nanoseconds
Network State	Milliseconds
Running Processes	Seconds
Disk	Minutes
Backup Medias	Years
CD-ROMS or printouts	Tens of years

Sometimes a small process trace can explain more than 50 gigabytes of a single backup...

Forensic Analysis - Theory - Layer(s)

- A computer system is a machine playing with the "treachury of images".
- An operation is often using one or more abstraction to be completed.
- The top-down approach of information from high-meaning to low-meaning is critical for forensic analysis.
- Computers become more and more mature but become less predictable at the row level.

Forensic Analysis - Theory - Layer(s) - The File System case

The file system is a great source of forensic information but :

- Forensic data must captured at the right layer. (e.g. using the tool of the file system is useful but not enough)
- Be prepare to collect partial information.
- File system analysis is often the next step after a detection. (e.g. from the network)
- File system analysis can be time consuming.

Forensic Analysis - General Practice

- First rule : Stay calm.
- Second rule : Limit risk but keep OOV in mind.
- Third rule : Never work on real data.

Forensic Analysis and Incident Response

- (Prevention)
- Detection
- Analysis
- Containment
- Investigation
- Eradication
- Postmortem

Forensic Analysis and Training

- The best way to be prepared for doing forensic analysis. It's to do it regularly.
- Participate to the reverse challenge of the honeynet project.
- Collect old filesystem and try to understand the last actions executed on the system.
- Prepare your legal staff to forensic analysis.

Bibliography

- Forensic Discovery, Dan Farmer, Wietse Venema, Addison Wesley ω
- Incident Response, Kenneth R. Van Wyk, O'Reilly
- Computer Forensics, Incident Response Essentials, Warren G. Kruse, Addison Wesley
- File System Foresinc Analysis, Brian Carrier, Addison Wesley
- Mechanisms, New Media and the Forensic Imagination, Matthew G. Kirschenbaum, The MIT press ω

Use case 1

- You have a public web server, hosted in a datacenter, that has been compromised (the main page has been defaced).
- The public web server also contains private information from the customer (mainly login and password).
- What should I do ?

Use case 2

- A laptop from a potential hostile employee has been given to you for analysis.
- What should I do ?

Use case 3

- You discovered a enterprise server with a proprietary software installed and doing unusual network connection to Internet.
- How forensic analysis could help me ?

Use case 4

- An employee gave you a flashcard where he would like to recover documents deleted ?
- How you would proceed ?

Q and A

- Thanks for listening.
- a@foo.be