Digital Forensics & Incident Response

Some information in these slides is based on presentations from various trainings - educational use only

Incident Response (“Incident Handling”)

“An action plan for dealing with the misuse of computer systems and networks”

-SANS

- Intrusions, insider threat
- Malware infections
- Theft, fraud
- Denial of Service
- Disaster recovery & business continuity
- Compliance

Why Incident Response?

- When incidents happen (not ‘if’) you want to be prepared
  - You could ignore it - bad
  - You could try to triage it - better
  - Have a documented procedure in place - best
- Legal requirements
  - Due care

Some information in these slides is based on presentations from various trainings - educational use only

What is an “Incident”?

- Deviation from the norm
- Harm or the attempt to harm

Examples

- Unauthorized use of an account
- Unauthorized use of a system
- Executing malicious code

Response

- Limit the damage
- Do not cause further damage
- Follow up remediation, prevention

Incidents are based on observable events

Some events may look malicious when they are legitimate, and vice versa

- System crash (could be normal behavior)
- Packet flooding (could be a legitimate burst of traffic)

Observable or tangible events are important to document

- Hold up well in court
- Record them in handwritten notebooks, cross-reference logs
- The same information gathered from multiple sources enforces validity

Questions?

Some information in these slides is based on presentations from various trainings - educational use only

6-Step Incident Handling Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Report (Lessons learned)

When considering steps to add to an IR plan consider:

“If an incident occurred, would I be thankful that I had done that?”

“Would I be really sorry if I hadn’t done that?”

Some information in these slides is based on presentations from various trainings - educational use only

Preparation

Get your team ready to handle incidents

- People - training
- Policy
  - Clearly defined, enforced (warning banners*)

Response strategies

- Maintain secrecy OR notify law enforcement
  - Notify if you are required to or can benefit from FBI assistance
  - Maintain to reduce downtime, publicity, risk of further hacking, affiliation with FBI
- Contain and clear OR watch and learn

We could get into emergency communications plans, jump bags, phone trees, etc. but that’s outside of the scope of this lecture.

Identification

- Gather evidence (events)
    - Network perimeter detections, Host perimeter detections, System-level detections, application-level detections
- Analyze them
- Determine a deviation from the norm and harm / the attempt to harm

Determine who is authorized to ‘pull the fire alarm’ or decide that an incident has been mitigated.

- Primary incident handler and helper

False alarms can be seen as training opportunities

Some information in these slides is based on presentations from various trainings - educational use only

Examples of ‘events’

Unusual…

- Processes, services
- Registry keys, scheduled tasks, startup items
- Network or memory usage
- Files, accounts
- Log entries

Be able to check for and identify the above on multiple systems

Chain of Custody

“Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence” - Thank you Wikipedia

- Maintain a provable chain of custody
  - Do not delete ANY files until the case is closed, even then try to save them for some retention timeframe
  - Identify every piece of evidence in your notebook
  - Control access to evidence
- Each piece of evidence must be under the control of one identified person at all times
  - Record handoffs: who and when, including when evidence is moved to storage
- When turning over evidence to law enforcement, have them sign for it

Some information in these slides is based on presentations from various trainings - educational use only

Containment, Eradication

Not going to go super in-depth, processes usually vary by incident details

- Stop the bleeding - prevent an attacker from further exploitation
- Secure the crime scene - similar to actual crime scene
  - Photos where applicable
  - Sometimes discrete
- Determine severity and sensitivity of incident
- Inform management and other involved parties
- Figure out short-term and long-term procedures - refer to IR plan!
- Eradicate - remove malware, restore backups, whatever you need to do

Don’t forget to document everything you do

Recovery, Report

Goal is to validate that the systems are normal and post-process any artifacts, come up with new prevention strategies

- Restore operations when feasible
- Monitor the systems
- Follow-up report as soon as possible
- Determine preventative fixes and apply them

Back to Preparation...

Common Mistakes, chronologically ordered

- Failure to report or ask for help
- Incomplete / non-existent notes
- Mishandling or destroying evidence
- Failure to create working images
- Failure to contain or eradicate
- Failure to prevent follow-on compromise months later
- Failure to apply lessons learned

Questions?

Some information in these slides is based on presentations from various trainings - educational use only

Digital Forensics

“Digital forensics ... is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.” - Thanks again Wikipedia

- Public / private sector careers
- Incident response roles

- Get to do work that assists in catching bad people
- Sometimes have to look at things that bad people do

Forensics is a science - relies a lot on the scientific method, reproducibility, and peer validation

Some information in these slides is based on presentations from various trainings - educational use only

Forensics Process

Depends on case

- Insider threat, theft, fraud investigation?
- System operating system / device

Always

- Maintain a proper chain of custody
- Copy and handle evidence in a forensically sound process
  - Use a write blocker when imaging drives
  - Keep a log of evidence, timestamps, people, etc.

Be aware of laws and legal processes

- Federal Rule 702
- Frye Standard
- The 4th Amendment in the Bill of Rights
- 18 U.S. Code § 1029 - Fraud and related activity in connection with access devices
- 18 U.S. Code § 1030 - Fraud and related activity in connection with computers
- Electronic Communications Privacy Act
- Digital Millennium Copyright Act

Some information in these slides is based on presentations from various trainings - educational use only

Questions?

Some information in these slides is based on presentations from various trainings - educational use only

File System Analysis

Most cases involve

- Recovering Deleted Files
  - How are files and directories stored?
  - What type of metadata is kept?
  - What happens when a files is deleted, modified, created, or accessed?
- NTFS (common file system Windows uses)
  - Everything in the filesystem is considered a file (including metadata)
  - All of this data is stored in the Master File Table (MFT)
    - Most recovery tools reference this when attempting to recover deleted files
    - Look for not in-use entries in the MFT to discover deleted files
  - Files of <700b are usually completely recoverable
    - Stored in the MFT itself, not overwritten when deleted
  - Larger files have a higher probability of having clusters overwritten

Some information in these slides is based on presentations from various trainings - educational use only

Other Categories of Analysis

- Volumen System analysis
- File Name Layer analysis
- Meta Data Layer analysis
- Data Unit Layer analysis

Each category has a defined way that data is stored and retrieved

- Forensics tools exist that operate at each layer
- We’re not going to go over them (out of scope)

Some information in these slides is based on presentations from various trainings - educational use only

File Carving

- Recovering files from an unstructured input
  - Hard drives
  - Network streams
  - Memory captures
- Useful when
  - You have some bitstream of data (mentioned above)
  - You need to recover all files without having a structured method to do so
  - The references to the files have been lost (they were deleted)
- Examples
  - A user downloaded/accessed a file they shouldn’t have and then deleted it
  - A user transferred malware onto a computer and then attempted to remove traces
  - I saved ten years worth of pictures on a USB drive and never backed it up

Some information in these slides is based on presentations from various trainings - educational use only

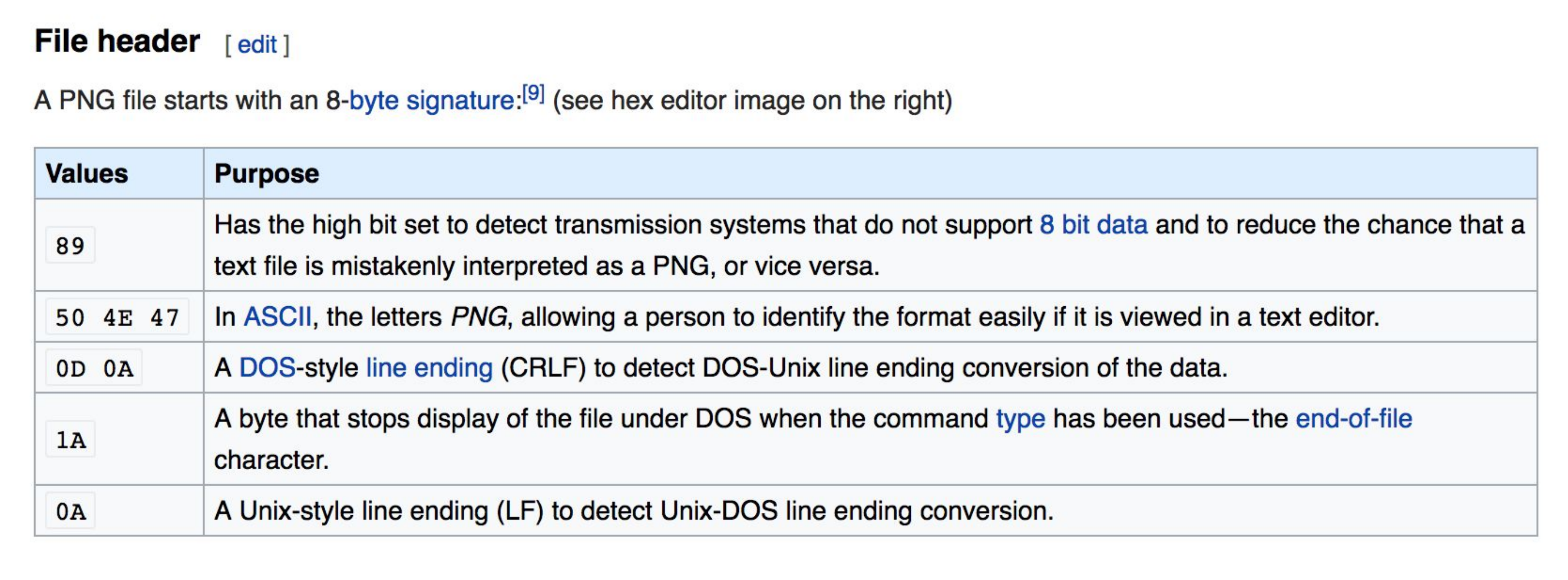
File Carving ..

Method 1: Header/Footer Searching

- All common file types have a standardized header, some also have a footer
- The carving tool has a database of these headers / footers
- Once a header is found, the matching footer is looked for within a range
  - Fast but false positives on file types with short headers/footers
  - Good at recovering partial files
  - Easy to add signatures for custom file types but does not work on files that do not have headers/footers

Method 2: Deep File Parsing

- Validates the data between the header/footer
- Few false positives but slow and needs constant updating



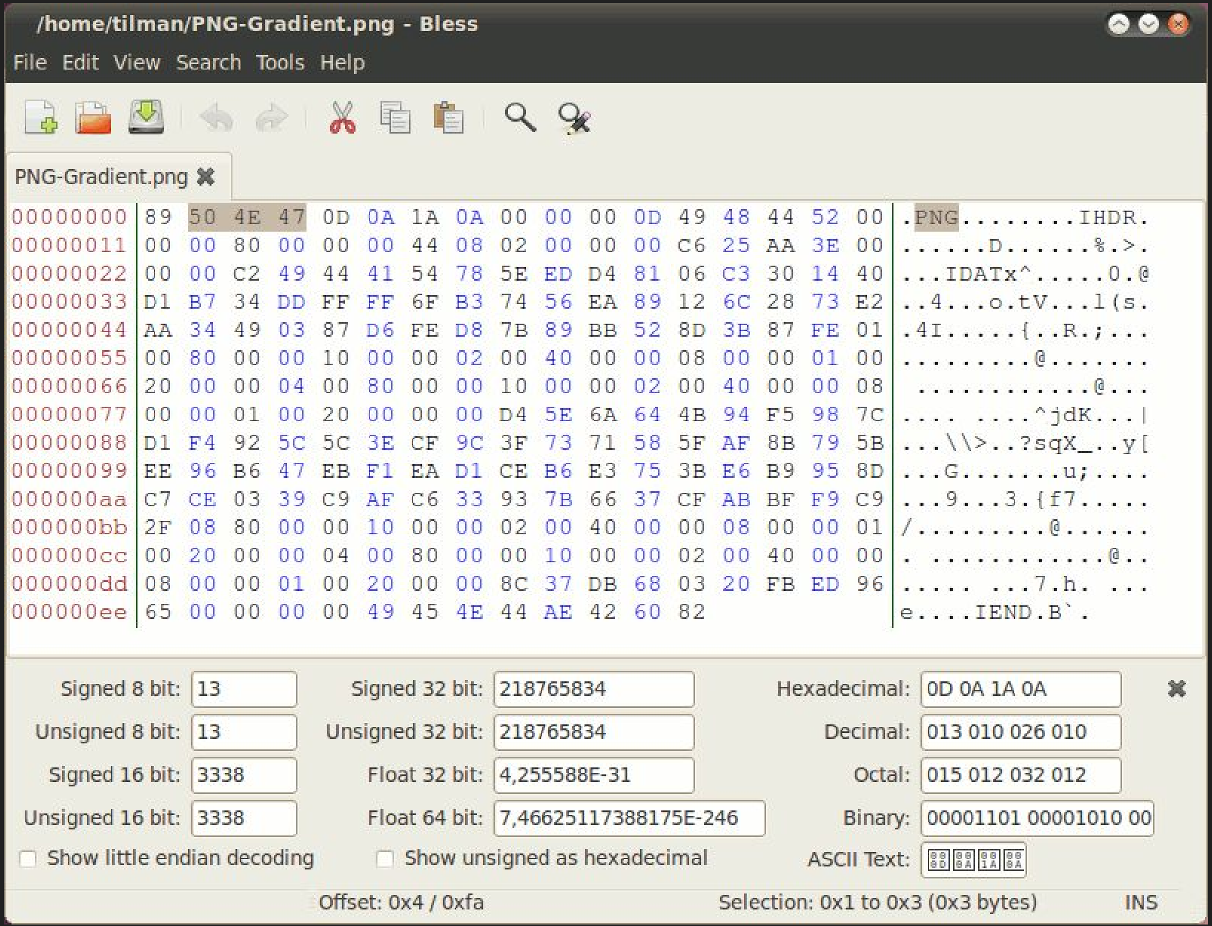
File header [edit]

A PNG file starts with an 8-byte signature:[9] (see hex editor image on the right)

Values	Purpose
`89`	Has the high bit set to detect transmission systems that do not support 8 bit data and to reduce the chance that a text file is mistakenly interpreted as a PNG, or vice versa.
`50 4E 47`	In ASCII, the letters *PNG*, allowing a person to identify the format easily if it is viewed in a text editor.
`0D 0A`	A DOS-style line ending (CRLF) to detect DOS-Unix line ending conversion of the data.
`1A`	A byte that stops display of the file under DOS when the command type has been used—the end-of-file character.
`0A`	A Unix-style line ending (LF) to detect Unix-DOS line ending conversion.

(Wikipedia)

Some information in these slides is based on presentations from various trainings - educational use only



/home/tilman/PNG-Gradient.png - Bless
File Edit View Search Tools Help
PNG-Gradient.png

```
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 .PNG........IHDR.
00000011 00 00 80 00 00 00 44 08 02 00 00 00 C6 25 AA 3E 00 ......D......%.>.
00000022 00 00 C2 49 44 41 54 78 5E ED D4 81 06 C3 30 14 40 ...IDATx^.....0.@
00000033 D1 B7 34 DD FF FF 6F B3 74 56 EA 89 12 6C 28 73 E2 ..4...o.tV...l(s.
00000044 AA 34 49 03 87 D6 FE D8 7B 89 BB 52 8D 3B 87 FE 01 .4I.....{..R.;...
00000055 00 80 00 00 10 00 00 02 00 40 00 00 08 00 00 01 00 .........@.......
00000066 20 00 00 04 00 80 00 00 10 00 00 02 00 40 00 00 08  ............@...
00000077 00 00 01 00 20 00 00 00 D4 5E 6A 64 4B 94 F5 98 7C .... ....^jdK...|
00000088 D1 F4 92 5C 5C 3E CF 9C 3F 73 71 58 5F AF 8B 79 5B ...\\>..?sqX_..y[
00000099 EE 96 B6 47 EB F1 EA D1 CE B6 E3 75 3B E6 B9 95 8D ...G.......u;....
000000aa C7 CE 03 39 C9 AF C6 33 93 7B 66 37 CF AB BF F9 C9 ...9...3.{f7.....
000000bb 2F 08 80 00 00 10 00 00 02 00 40 00 00 08 00 00 01 /.........@......
000000cc 00 20 00 00 04 00 80 00 00 10 00 00 02 00 40 00 00 . ............@..
000000dd 08 00 00 01 00 20 00 00 8C 37 DB 68 03 20 FB ED 96 ..... ...7.h. ...
000000ee 65 00 00 00 00 49 45 4E 44 AE 42 60 82             e....IEND.B`.
```

Signed 8 bit: 13
Unsigned 8 bit: 13
Signed 16 bit: 3338
Unsigned 16 bit: 3338
Signed 32 bit: 218765834
Unsigned 32 bit: 218765834
Float 32 bit: 4,255588E-31
Float 64 bit: 7,46625117388175E-246
Hexadecimal: 0D 0A 1A 0A
Decimal: 013 010 026 010
Octal: 015 012 032 012
Binary: 00001101 00001010 00
ASCII Text:

☐ Show little endian decoding ☐ Show unsigned as hexadecimal

Offset: 0x4 / 0xfa Selection: 0x1 to 0x3 (0x3 bytes) INS

Some information in these slides is based on presentations from various trainings - educational use only

Anti-Forensics

- As an investigator we want to be able to know when anti-forensics is in use
- And also prove that anti-forensics was used
  - Destruction of evidence in legal matters
  - Will also justify why your report has none of the usual findings
- Most tools outright delete data if possible
  - Or modify it in place if it can’t be deleted
  - Some data can’t be deleted
    - Restore Points
    - Volume Shadow Copies
    - Registry Hives (Deleted Keys)
- Leverage leftover artifacts from scrubbing tools

TL;DR

Information on files is stored in a lot of places

Deleting just the file is not sufficient for destroying evidence

Lots of other cool things we don’t have time to talk about…

- Information is stored on the OS when you plug in removable media
  - Makes it possible to do forensics on a USB without having the USB
- On low-use computers, files can be recovered years after they are deleted
- Memory forensics and network forensics have additional unique tools & processes

Forensics isn’t usually as glamorous as it looks on TV.

Additional Reading / Resources

SANS Incident Response Forms

NIST Computer Security Incident Handling Guide

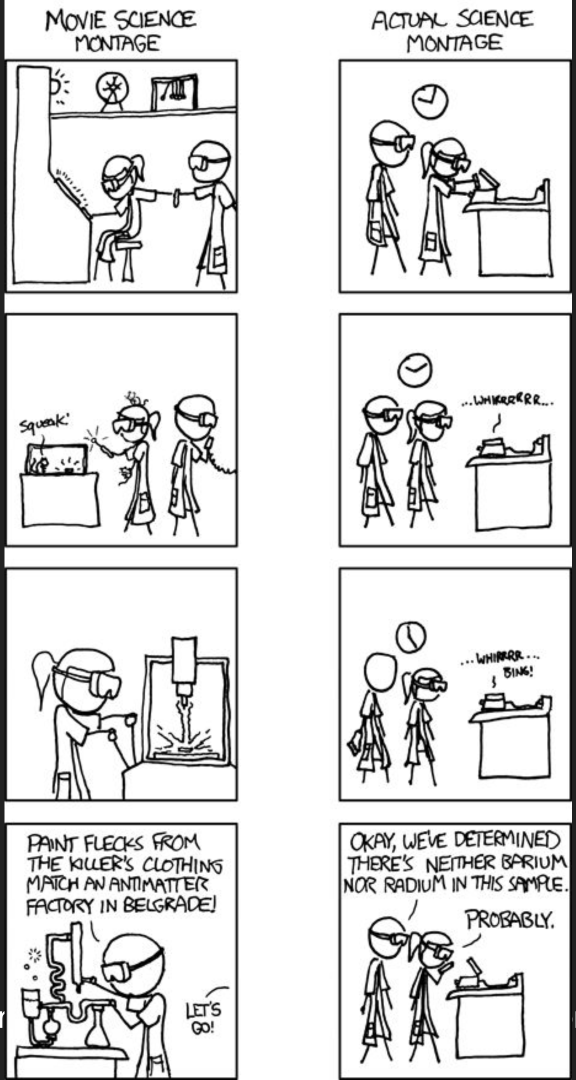
SANS Internet Storm Center blog

Forensics Wiki

File System Forensics Analysis book

Some information in these slides is based on presentations from various trainings - educational use only

Obligatory XKCD Comic


MOVIE SCIENCE MONTAGE
ACTUAL SCIENCE MONTAGE
squeak!
...WHIRRRRRR...
...WHIRRRR...
BING!
PAINT FLECKS FROM THE KILLER'S CLOTHING MATCH AN ANTIMATTER FACTORY IN BELGRADE!
LET'S GO!
OKAY, WE'VE DETERMINED THERE'S NEITHER BARIUM NOR RADIUM IN THIS SAMPLE.
PROBABLY.

Some information in these slides is based on presentations fr nly