SWINBURNE UNIVERSITY OF TECHNOLOGY

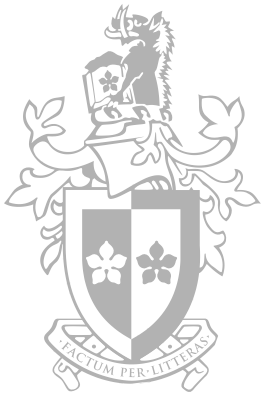
ICT30010 eForensic Fundamentals

Lecture 4

Forensic Report Writing

Troy Pretty

Digital Forensic Analyst



SWINBURNE UNIVERSITY OF TECHNOLOGY

Outline and learning goals

- Chain of Custody/Authentication
- Purpose
- Audience
- Report Types
- Report Content
- Lab Reports

Chain of Custody

- Process of dealing with and handling evidence
  - Where, when and by whom evidence collected
    - Physical transfer/online download
  - Where, when and by whom evidence handled or examined
  - How evidence was stored and who had access to it
  - Document any transfer of custody
- Accountability of evidence while in your control
- Unexplainable “breaks in the chain” can result in evidence being discounted

Authentication

- Hash functions are use for authentication
  - Whole disk
  - Individual partition
  - Individual item
- 3rd Party provides a forensic image and hash
  - Validate correct item has been received
  - Validate that item is not corrupt
- Validate that item is unchanged after an investigation
- Validate or locate items of interest

Report Purpose

- Present the findings of a forensic analysis
  - Outline processes followed
  - Present the evidence located
- Stick to the facts
  - Non biased
- Appropriate for the target audience

Audience

- Lawyers
- Courts
- Employers / Clients
- Forensic Professionals

Lawyers

- Related to criminal investigations
- Prosecution
  - Interested in pressing charges
- Defence
  - Defending an accused
- Rely on reports to understand if there is/isn't enough evidence to support charging a person

Courts

- Once a matter has gone to trial
  - Judge
  - Magistrate
  - Jury
- Help show if a person of innocent or guilty of offence
- Often require forensic professional to attend and present evidence

Employers / Clients

- Related to incident response or HR investigations
- Part of your role
- Contracted by a client
- Interested in the following:
  - Was a server hacked
  - Was data stolen
  - How did the event occur
  - How can it be prevent
  - Remediation

Forensic Professionals

- Peer Review
  - Check for accuracy
  - Check to ensure process have been followed
- Defence Experts
  - Looking for holes in you processes
  - Is the evidence correct
  - Has evidence been planted

Report Types

- Case Notes
- Artifact
- Automatically Generated
- Forensic Case Report
- Statement

Case Notes

- Not directly a forensic report type
  - Content forms the basis of a forensic report
- Continuity of the exhibit
- Observations
  - Exhibit
  - Date/Time/Timezone
- Chronological timeline of forensic tasks
- Results from forensic processes
- May contain content that doesn't appear in a forensic report
- Can be called upon as evidence

Artifact Report

- Quickly identify items of interest
  - User files
  - Log records
- Used to quickly present preliminary findings
- Highlight further avenues of enquiry
- Often printed
- Lacks context

Automatically Generated

- Automatically generated from a forensic tool
- Includes all items
  - Relevant
  - Irrelevant
- Investigator needs to review to find evidence
- Privacy issues
- Often 100's or 1000's of pages long
- Examples:
  - Full internet history
  - Full mobile phone extraction

Forensic Case Report

- Scope of analysis
- Tools used
- Assumptions/Limitations
- Process taken
- Results/Findings
- Conclusion/Remediation

Statement

- Outline your qualifications/experience
- Continuity
  - How item was received
  - How it was verified
  - How it was stored
- Tells the story about your involvement
- Outlines your findings
- Contains only facts
- Sworn statement
  - If caught making false statement can face perjury charges

Report Content

- Stick to the facts
  - Don’t make up stories
- Incorrect:
  - Fred downloaded an illegal file on Friday at 8:30pm
- Correct:
  - I located a file that was downloaded to the computer on Friday at 8:30pm

Report Content

- Only talk about the work you completed
  - If you didn't create the forensic image, you cant talk about how it was created or its source
  - Multiple forensic professionals may need to produce reports
- Incorrect:
  - On the 12/02/2017 John created a forensic image of the computer using FTK Imager and then handed the image to me on the 13/02/2017.
- Correct:
  - On the 13/02/2017 John provided me a forensic image file named "USB drive.dd"

Report Content

- Find a balance
  - Enough detail so the results can be reproduced
  - Not too technical, don't want to confuse people
- Incorrect:
  - I ran the comment istat –o 63 lab3.dd 123
- Correct:
  - I used a forensic tool and recovered a deleted file, the details of the recovered file are as follows:

Report Content

- Artifact Meta Data
  - Name of the item
  - Full path
  - Sector location, inode number
  - File size
  - Dates and Times
    - Created, Written, Accessed
  - GPS Co-ordinates
  - Camera make/model
  - Author

Report Content

- Dates and Times
  - Document and understand timezone
    - UTC
    - AEST/AEDT
  - Report on the full date and time down to second/millisecond
  - The incorrect timezone or a few seconds is the difference between some one being innocent or guilty.

Report Content

- Relevant Content
  - Don’t include 5 years of internet history if only a handful of entries are relevant
    - Include the relevant entries in the body of the report
    - Consider referencing the entire report in an appendix

Report Content

- Report Layout
  - The use of short dot points make the report easy to follow
  - The use of tables is highly recommended
- Hard to read:
  - I recovered 2 deleted files named file1.doc located at sector 45 and file2.doc located at sector 87. The created time for both files is 09:37am on the 17th of Feb 2016
- Easy to read:
  - I recovered 2 deleted files, their details are as follows:

Name	Sector	Date	Time
File1.doc	45	17/02/2016	09:37am
File2.doc	87	17/02/2016	09:37am

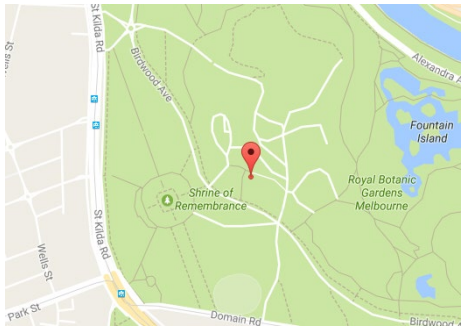
Report Content

- Screenshots
  - Use only where required
  - Never include a screenshot without making comment about it
    - Explain why it is relevant
    - Don’t make comments such as “the evidence is in the screenshot”
  - Make sure the screenshot is easily viewable when printed

Report Content

- Complete and accurate data/findings
  - Don’t summarise or roundup values
- Incorrect:
  - -37,144

- Correct:
  - -37.830000,144.975833



Report Content

- Format results and provide context
- Incorrect:

"1","0.000017","Vmware_46:2a:7e","Vmware_c0:24:2b","ARP","42","192.168.28.1 is at 00:0c:29:46:2a:7e"
"2","0.000304","192.168.28.2","192.168.28.1","ICMP","74","Echo (ping) request id=0x0200, seq=768/3, ttl=128"

- Correct

No.	Time	Source	Destination	Protocol	Length	Info
1	8:20:01	Vmware_46:2a:7e	Vmware_c0:24:2b	ARP	42	192.168.28.1 is at 00:0c:29:46:2a:7e
2	8:20:02	192.168.28.2	192.168.28.1	ICMP	74	Echo (ping) request id=0x0200, seq=768/3, ttl=128

Lab Reports

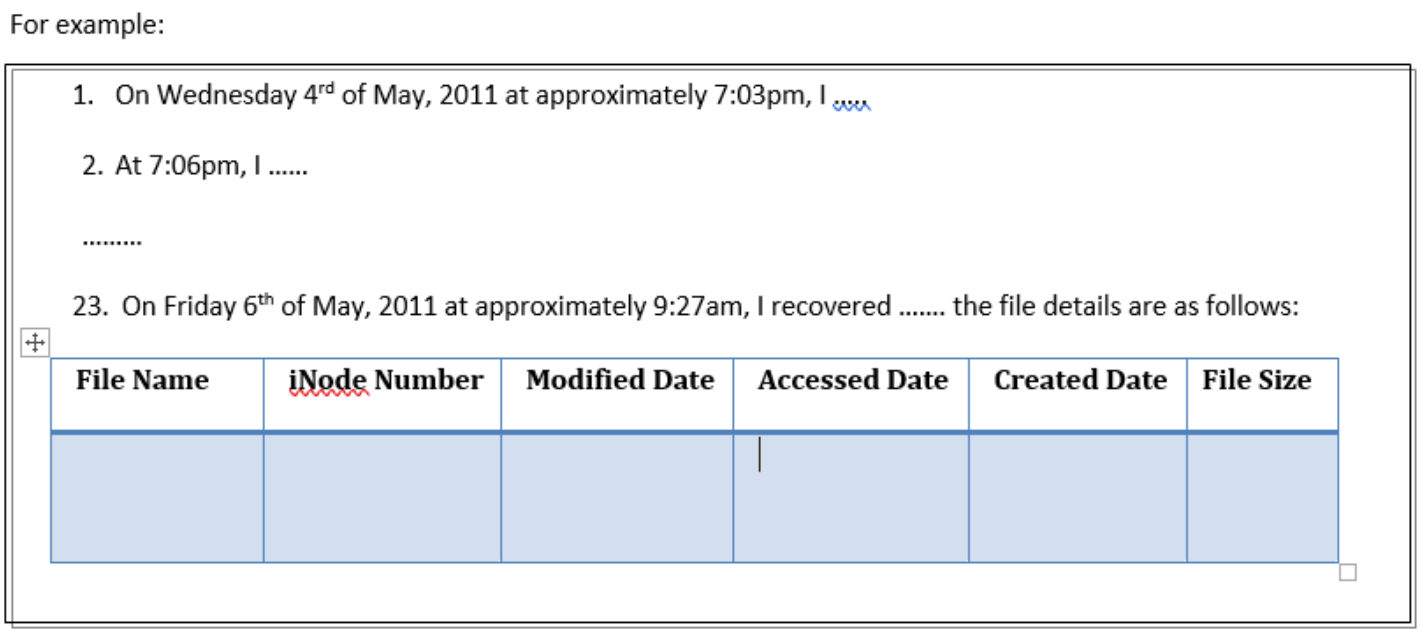
- Read section 7 of the lab scenario, it outlines what is required.
- Understand the marking scale, it outlines where the marks are allocated.
- If you rely on any outside material in your reports ensure it is referenced
  - Referencing conventions required for this unit are: Author-Date or IEEE.

Lab Reports

- Layout is entirely up to you
  - A combination of the forensic case report and a statement is most appropriate
  - Dot points and tables are good
  - Minimal screenshots
- Stick to the facts
- Ensure your report is easy to read but includes enough relevant information
  - A forensic professional should be able to reproduce the same results
  - A non technical person should be able to understand the results

Lab Reports

- Page 15 of Lab 3 contains a brief example



For example:

1. On Wednesday 4rd of May, 2011 at approximately 7:03pm, I ....

2. At 7:06pm, I .....

.....

23. On Friday 6th of May, 2011 at approximately 9:27am, I recovered ..... the file details are as follows:

File Name	iNode Number	Modified Date	Accessed Date	Created Date	File Size

Reference

SANS - Intro to Report Writing for Digital Forensics

https://www.sans.org/blog/intro-to-report-writing-for-digital-forensics/