The Value of Contemporaneous Notes and Why They Are a Requirement for Security Professionals

GIAC (GCIH) Gold Certification

Author: Seth Enoka, seth.enoka@gmail.com
Advisor: Chris Walker

Accepted: September 5th, 2019

Abstract

Contemporaneous notes, or notes taken as soon as practicable after an event or action takes place, are invaluable to analysts in security roles performing activities such as digital forensics and incident response. There are various situations where contemporaneous notes provide a disproportionate return on time invested. However, there is no standard which defines the minimum information to record or indicates why every analyst should create some form of contemporaneous notes, whether in the civil or criminal domain. Timestamping, "write-once" versus write-many modalities, and how to edit or amend contemporaneous notes are important considerations. Additionally, including enough information such that the analyst, or any analyst, can follow the notes after time has elapsed and still achieve the same results and conclusions is essential when taking contemporaneous notes. The evidentiary value of contemporaneous notes should be defined and understood by every security professional.

1. Introduction

Note-taking is a critical part of working as a security professional. Notes often form the basis of successful investigations (Professional Note Taking, 2007). Regardless of whether the task being performed is proactive or reactive, the nature of the security industry necessitates diligent creation of contemporaneous notes (CN). In some jurisdictions, the taking of notes and the information which must be recorded is defined by legislation (Notebook Guidance, 2017), and it behooves the security professional to know if this service is provided.

Some security professionals do not believe in taking notes. This position is taken up for a number of reasons, such as the perception that there is no time while performing digital forensics and incident response related activities. Otherwise, no one else in their peer group takes notes, so it is not believed to be an important part of the role (Shavers, 2018).

On the contrary, creating contemporaneous notes is an integral part of and tool in any security professional's toolkit. Those who fail to take notes will eventually land in a position where had they taken notes while performing their duties they would be in a much better position than they otherwise find themselves (Notebook Guidance, 2017).

Contemporaneous notes need not be created as security activities occur, although this would be ideal; by definition, they should be taken as soon as possible following an action. However, due to the fragility of human memory, it is in the best interests of all involved in a security engagement that contemporaneous notes be created (Professional Note Taking, 2007).

There are several reasons this is the case. The first is the fact that notes are often relied upon months or years after an engagement has been completed. The second is that any engagement has the potential to lead to litigation. These are just two prime examples (Guidance on Keeping of Contemporaneous Notes, n.d.). Notes can be taken in many forms, including physically, electronically, or video- or photographically (Trewmte.blogspot.com, 2018). Given the many and varied ways of recording information contemporaneously, there can be no excuse given for not taking contemporaneous notes.

2. Why Contemporaneous Notes Must Be Taken

Contemporaneous notes should be taken during any engagement where the possibility exists that the notes may be later required. Human memory is similar to RAM; it is volatile and easily corrupted over time (Professional Note Taking, 2007). The longer the period between an analyst (which here refers to anyone performing security activities as an investigator, a consultant, or in any other role) performing an action during an engagement and notes related to that action being created, the higher the chance of misremembering, or worse, completely forgetting, what was done or found. Flawed, inaccurate recollection poses considerable risk to the analyst and the organisation if the validity of their work or findings are later questioned (Shavers, 2018).

It is equally as essential to take CN during triage (reactive) activities such as compromise assessment as it is in structured digital forensics (reactive) and incident response (DFIR) or malware analysis. Triage (proactive) activity has the potential to turn into or form part of a DFIR investigation. In these cases, it is better to have as much information as possible related to the activities that justify the need for DFIR.

When a reactive DFIR engagement starts, there is an even greater need to begin the note-taking process promptly, i.e. from the first contact with the stakeholder(s). This ensures that as much detail as possible about the event or incident are recorded. These notes need to be referred to throughout the engagement. As the engagement progresses, the analyst(s) should continue to take notes in such a way that they, or any other analyst, could follow the same process and achieve the same results and findings at any point in the future. Attempting to reproduce results and findings without notes taken at the time of the original analysis is very difficult as circumstances are difficult to replicate (Shavers, 2018).

Having comprehensive CN is also of value when it comes time to write the report and brief the stakeholder(s) on the outcome and findings of the engagement (Shavers, 2018). Trying to write a report from memory when most of the work was performed even in the recent past is an arduous and painful task.

Notes of any kind are particularly useful once engagements are complete and during lessons learned exercises (Professional Note Taking, 2007). They can be used to identify issues which arose during an engagement, which should then feed into process improvement. Having notes relating to how issues encountered can be resolved is useful for knowledge sharing between team members and for new or junior members of a team.

Additionally, if a team member is unavailable, any other member of the team should be able to follow their notes and continue working on the engagement in their absence. This transparency allows a team to work as efficiently as possible, resulting in better outcomes and lower time to remediate in the case of incident response.

3. Who Should Take Contemporaneous Notes?

Given the importance of note-taking, taking CN should be an organisational policy which applies to all analysts, rather than a guideline or recommendation. Every analyst should take CN. This should form part of every analyst’s job description. Organisations have chosen to terminate analysts who fail to keep contemporaneous notes, especially when issues arise from failing to do so.

Comprehensive CN protect both the note taker and their organisation in the event of adverse outcomes or legal action resulting from actions taken (or not taken) by the analyst. Moreover, an analyst being able to refer their own CN in court, during a deposition, or any other such situation, is invaluable (Notebook Guidance, 2017). The closer to the action the notes are created and the more detailed they are, the more credible they, and the analyst, are likely to be considered.

4. When to Take Contemporaneous Notes

Contemporaneous notes, by definition, are created as soon as possible after an action or event has taken place (Notebook Guidance, 2017). By contrast, simultaneous notes (SN), are taken at the same time as an action or event, as in the case of photo or video records (Trewmte.blogspot.com, 2018). For example, if an analyst runs a shell command and immediately copies that command and the subsequent output to their notes, this would be considered SN. Running the command at the beginning of the day and recording the output at the end of the day would be considered to be CN.

In most cases, notes taken at the same time as or closely following actions are likely to be more accurate and complete than notes taken much later (Newswise.com, 2018). Ipso facto, CN taken as close to the action or event as possible are preferable, and are considered more credible (Professional Note Taking, 2007).

While SN would be considered more credible and preferable to CN, taking CN is sometimes more realistic. However, SN can be more convenient, as in the case of shell commands. When an analyst is taking their notes electronically, it is more convenient for the analyst to immediately copy both the command and related output from the command-line interface (CLI) into their notes. Conversely, trying to backtrack at a later stage can lead to information being lost and therefore not recorded, potentially leading to wasted time, duplication of effort and forgotten findings.

If notes cannot be taken while working, it is acceptable to take notes of actions, observations, and outcomes at a later stage. Notes taken within days following a forensic examination, for example, may still be considered contemporaneous. Other message formats are acceptable and have been accepted in the past, including text messages and email sent during the event. For the sake of accuracy and completeness, take notes during or immediately after the proactive or reactive response.

5. How to Take Contemporaneous Notes

Physical or electronic notebooks, as well as photo and video, are all valid methods of taking CN (Trewmte.blogspot.com, 2018). Considerations need to be made regarding convenience and integrity when choosing a method, and a combination of methods may be necessary depending on the given situation.

Firstly, an analyst needs to determine how to maintain the integrity of the CN. Leaving the integrity of the notes open to question diminishes their value. Use a write-once method that cannot be altered once the notes are taken. Taking notes in a physical notebook using a permanent pen is the best approach. Alterations are self-evident and subject to confirmation.

The biggest concern with write-once record-keeping methods is that small but necessary changes, such as grammar, spelling, or corrections, cannot be made. In most cases, if there is an auditable mechanism for making such amendments, this does not pose a problem. Alternatively, amendments can be taken in a separate note and attached as an appendix or appended as errata (Notebook Guidance, 2017).

If taking notes electronically, using a tool which maintains strict versioning, such as Confluence or JIRA (Appendix C), may be an option. Any system of note-taking that is auditable and keeps track of changes made after the fact can be used to successfully maintain the integrity of CN (Trewmte.blogspot.com, 2018). Applications such as Evernote (https://evernote.com/) or Forensic Notes (https://www.forensicnotes.com/) are available for multiple operating systems and allow for note history and versioning.

One further option for maintaining the integrity of electronically taken CN is to hash the notes once they are complete (Trewmte.blogspot.com, 2018), such as at the end of each examination session or the end of each examination day. The notes can then be hashed again at a later date and the hashes compared to ensure that the notes have not changed since being taken. Notes and their hashes should be stored separately in such a way that the hashes cannot be modified. If both the notes and the hashes can be modified, the integrity is lost.

Physical notebooks are a tried and true method of taking CN. If used correctly, physical notes have high integrity and credibility. When taking notes in a physical notebook, there are some rules to follow (Notebook Guidance, 2017). First of all, ensure that the notes are legible; otherwise, they are of little value. Physical notes should be taken in pen, and whiteout or similar should not be used. This protects their integrity. If errors are made during note-taking, the erroneous note(s) should be marked as deleted but not removed, i.e. a single strike-through, and amendments noted and initialled or errata appended (Professional Note Taking, 2007). Pages should never be torn out of notebooks. This is assumed to be malicious redaction. There should be no large blank spaces which would allow for later additions (Professional Note Taking, 2007). Finally, physical notes should not be taken on scrap pieces of paper, and should instead be taken in a bound notebook or notebooks (Guidance on Keeping of Contemporaneous Notes, n.d.). Unbound notes leave it up to the imagination how many other pieces of paper have not been recovered or presented, similar to tearing pages from bound notebooks. An example of physical notes is included in Appendix D.

Photos and videos can capture information quickly, such as the output of commands or the state of a scene or system where evidence is found or collected (Professional Note Taking, 2007). They also contain reliable metadata such as date and time data, or geolocation information. The drawback: they can capture more information than the analyst intended, such as conversations occurring between analysts which are irrelevant or damaging (while still not being relevant to the matter at hand) in the case of video. Use caution when taking photos or capturing video to prevent irrelevant (or impeachable) material from being captured, especially when there are not written or typed notes.

6. What Should Contemporaneous Notes Include

The contents of CN are one of the most subjective aspects of any engagement. At a minimum, notes should include: actions taken, including a time and place; commands run and their output; results and findings (Notebook Guidance, 2017). After the fact, any analyst should be able to follow the notes and arrive at the same results and findings. Examples of acceptable contemporaneous notes are shown in Appendices C and D.

Timestamping of notes is good forensic practice as it allows analysts to identify any activity on a system which can be attributed to themselves rather than the user or owner of that system (Guidance on Keeping of Contemporaneous Notes, n.d.). At the least, note the start and end date and time of an examination. These notes will be used after an engagement to justify time spent. Any gaps in coverage, such as breaks, should also be recorded. This provides a holistic view of when actions were taken.

If the event encompasses multiple locations, note where the notes were taken (Notebook Guidance, 2017). This includes, for instance, on-site, the analyst's headquarters. Moreover, this allows evidence locations to be verified after the fact. Pertinent details such as the evidence name, number, description, and other important details should be included in the notes.

For CN, include actions and the systems on which they were taken. (Professional Note Taking, 2007). Without this information, engagement findings may be impossible to reproduce. The integrity of the evidence will be affected by this omission since it cannot be attributed to either the owner of the system or the analyst. This extends to commands run on a system; the command itself should be recorded in its entirety, as should the output of the command.

Findings and observations should be recorded as and when they arise and should be stated in a matter of fact manner (Guidance on Keeping of Contemporaneous Notes, n.d.). Include all known information related to the findings. This includes where the information was found, time/date, and the user or owner details, as well as the software or method used (Shavers, 2018). Do not record inferences and assumptions except to provide context for actions taken. Hypotheses and facts confirming or refuting these should be noted as well.

When using abbreviations, they should be defined at their first use, i.e.:

A Refined Volume Snapshot ***(RVS)*** *was taken in X-Ways Forensics v19.8* ***(XWF)****.*

All programs used, including their versions, must be recorded. Later versions of software used for the analysis may provide different, or additional, results and findings.

Contemporaneous notes should be detailed and granular enough that the analyst or anyone else can follow the same process and arrive at the same findings or conclusions (Shavers, 2018). More information is better than less, and it is always better to have information and not need it rather than need it and not have it. If questioned later as to the provenance of evidence or findings, it is always better to have as much information as possible, rather than rely on memory (Newswise.com, 2018). If an action is taken and not recorded, this can lead to later issues. Conversely, it is more often than not possible to explain why a particular action was or was not taken in an exculpatory manner if related notes exist; if they do not the analyst may be in a worse position for lack of those notes.

Also note engagement-related communication (Notebook Guidance, 2017). These notes should include the time, location, medium, and persons involved in the conversation. If the communication was by phone, it is best to try to take notes of the conversation during or immediately after the call concludes (Professional Note Taking, 2007). Following up with an email is a suitable method for maintaining a record which is discoverable and can form part of the analysts CN.

7. Conclusion

Every security professional, especially those performing digital forensics and incident response or related proactive activities, should take contemporaneous notes. This practice is in not only their own best interests but those of their employers and their stakeholders as well. The ability to take concise, complete, and accurate notes of actions taken during an engagement should not be underestimated and should form part of the standard operating procedures of any security team or firm.

Since the security industry has strong affinity and affiliation with the legal industry, and other high stakes verticals such as finance and insurance, contemporaneous notes should be insisted upon by stakeholders on all sides. While there is no standard method or list of required information when it comes to note-taking, and arguably there should not be as it would be too onerous and subjective, decision-makers are urged to require contemporaneous notes. The inherent risks of not taking notes are too significant to ignore.

References

Notebook Guidance. (2017). 8th ed. [pdf] Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808533/notebook-guidance-v8.0extarchived.pdf [Accessed 2 Aug. 2019].

Guidance on Keeping of Contemporaneous Notes. (n.d.). [pdf] Transport Development & Solutions Alliance. Available at: http://www.tdsa.org.au [Accessed 2 Aug. 2019].

Professional Note Taking. (2007). [pdf] Rosanna, Victoria: Custom Training Network. Available at: https://www.is.vic.edu.au/static/uploads/files/note-taking-wfgzsotttytv.pdf [Accessed 2 Aug. 2019].

Newswise.com. (2018). Law Professor Explains the Hierarchy of Evidence and How Contemporaneous Notes Would — or Wouldn't — Hold up in Court. [online] Available at: https://www.newswise.com/articles/law-professor-explains-the-hierarchy-of-evidence-and-how-contemporaneous-notes-would-%E2%80%94-or-wouldn%27t-%E2%80%94-hold-up-in-court [Accessed 2 Aug. 2019].

Trewmte.blogspot.com. (2018). What's happening with Contemporaneous Notes. [online] Available at: https://trewmte.blogspot.com/2017/07/whats-happening-with-contemporaneous.html [Accessed 2 Aug. 2019].

Shavers, B. (2018). Brett's opinion on DFIR notes and note-taking. [online] Brettshavers.com. Available at: https://brettshavers.com/brett-s-blog/entry/brett-s-notes-on-note-taking [Accessed 26 Jul. 2019].

Appendix

A. Glossary of Terms

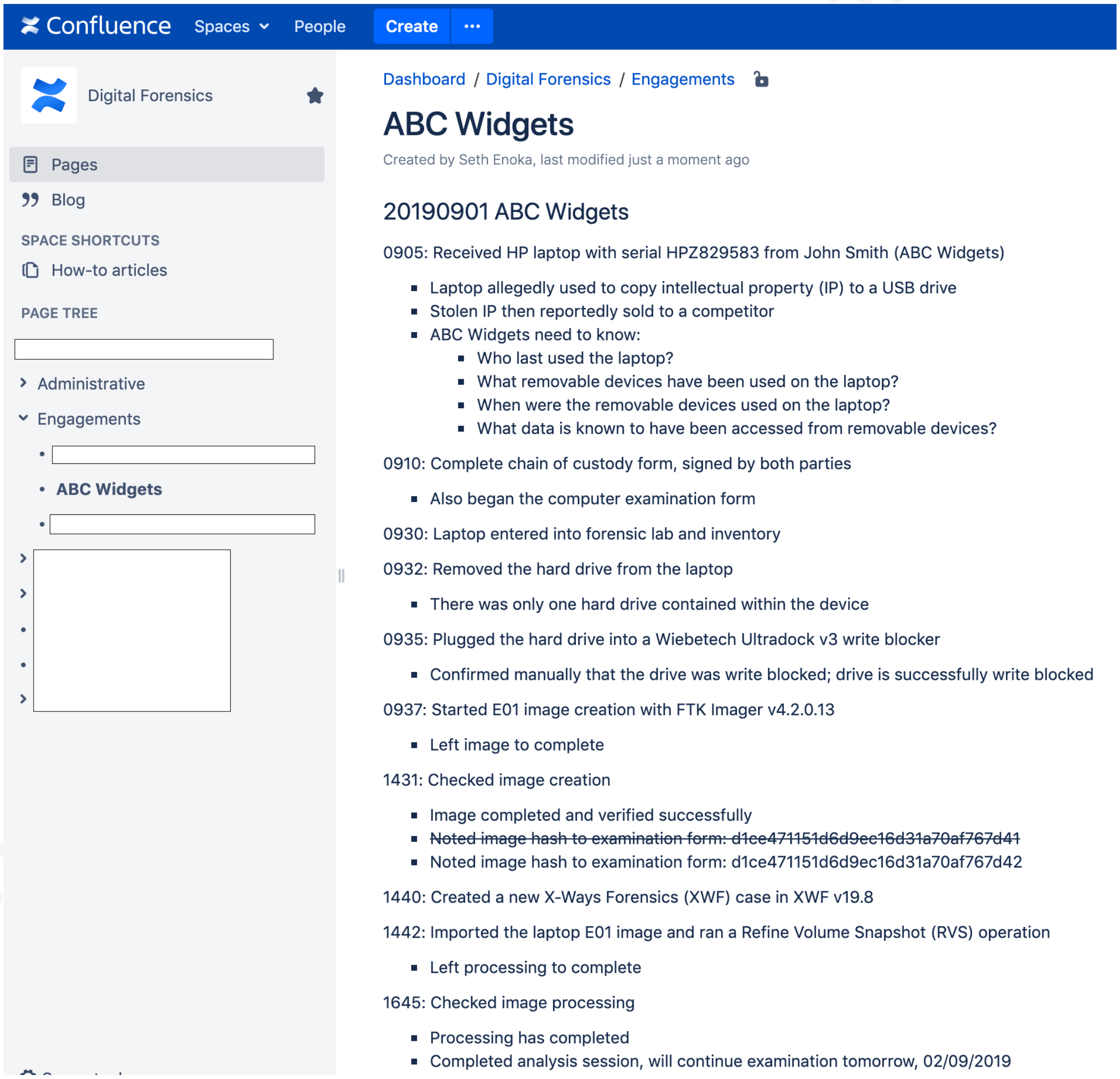
Term	Definition
Contemporaneous Notes (CN)	Notes made at the time or shortly after an event or action occurs.
Simultaneous Notes (SN)	Notes made at the same time an action occurs, i.e. a photo or video.
DFIR	Digital Forensics and Incident Response.
Analyst	Any person performing security activities as an investigator, a consultant, or in any other role.

B. List of Data Useful to Record (Non-Exhaustive)

Term	Definition
Date and time	Date and time should be recorded when the analyst arrives at or departs a location where work is to take place. Temporal information should additionally be recorded whenever work is started or stops, including the reason (i.e. lunch break). If noted at the time of the action, just the actual date and time are sufficient. If noted later, the date and time of the note being created should also be recorded.
Location	The location of the action being noted should also be recorded. If taking notes while on-site, the site location itself is recorded. If taking notes after the fact, the location of the activity and the location of the note-taking should be recorded.
Stakeholders present or involved	Anyone who is present while work is being performed should be noted. If anyone is conspicuously absent, this should likewise be noted.
Medium (of communication)	When communication takes place between the analyst and other stakeholder(s), this communication should be recorded in contemporaneous notes, including the medium of communication, i.e. phone, email, etc.
Evidence	When capturing details of evidence either observed or collected, as much detail as possible should be noted. Details such as evidence name, evidence number, description, distinguishing features, etc. are very useful during an engagement, and when reviewing for reporting.
Case details	If there are case or matter details, it is beneficial to record these to help identify to what the notes relate. Case or matter numbers, names, and details are useful.
Any details observed or obtained, anything seen, heard, or otherwise found	Ideally, details about the issue at hand will make up the bulk of an analyst's contemporaneous notes. As much detail as possible should always be recorded.

C. Example: Contemporaneous Notes (Confluence, Brief)

The image below is an example of contemporaneous notes which could be taken during a forensic investigation. This example is purposely short for the sake of brevity but is intended to give an indication of how and what an analyst should record.



ABC Widgets

Created by Seth Enoka, last modified just a moment ago

20190901 ABC Widgets

0905: Received HP laptop with serial HPZ829583 from John Smith (ABC Widgets)

- Laptop allegedly used to copy intellectual property (IP) to a USB drive
- Stolen IP then reportedly sold to a competitor
- ABC Widgets need to know:
  - Who last used the laptop?
  - What removable devices have been used on the laptop?
  - When were the removable devices used on the laptop?
  - What data is known to have been accessed from removable devices?

0910: Complete chain of custody form, signed by both parties

- Also began the computer examination form

0930: Laptop entered into forensic lab and inventory

0932: Removed the hard drive from the laptop

- There was only one hard drive contained within the device

0935: Plugged the hard drive into a Wiebetech Ultradock v3 write blocker

- Confirmed manually that the drive was write blocked; drive is successfully write blocked

0937: Started E01 image creation with FTK Imager v4.2.0.13

- Left image to complete

1431: Checked image creation

- Image completed and verified successfully
- ~~Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d41~~
- Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d42

1440: Created a new X-Ways Forensics (XWF) case in XWF v19.8

1442: Imported the laptop E01 image and ran a Refine Volume Snapshot (RVS) operation

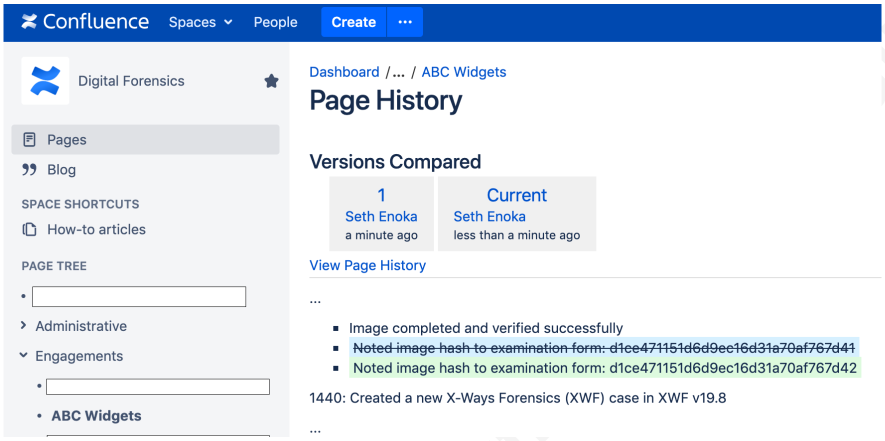
- Left processing to complete

1645: Checked image processing

- Processing has completed
- Completed analysis session, will continue examination tomorrow, 02/09/2019

Figure 1: Contemporaneous Notes in Confluence

Given that Confluence keeps an audit trail of pages when changes are made, no initials or timestamp are required for the altered hash at 14:31, as evidenced here:



...

- Image completed and verified successfully
- ~~Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d41~~
- Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d42

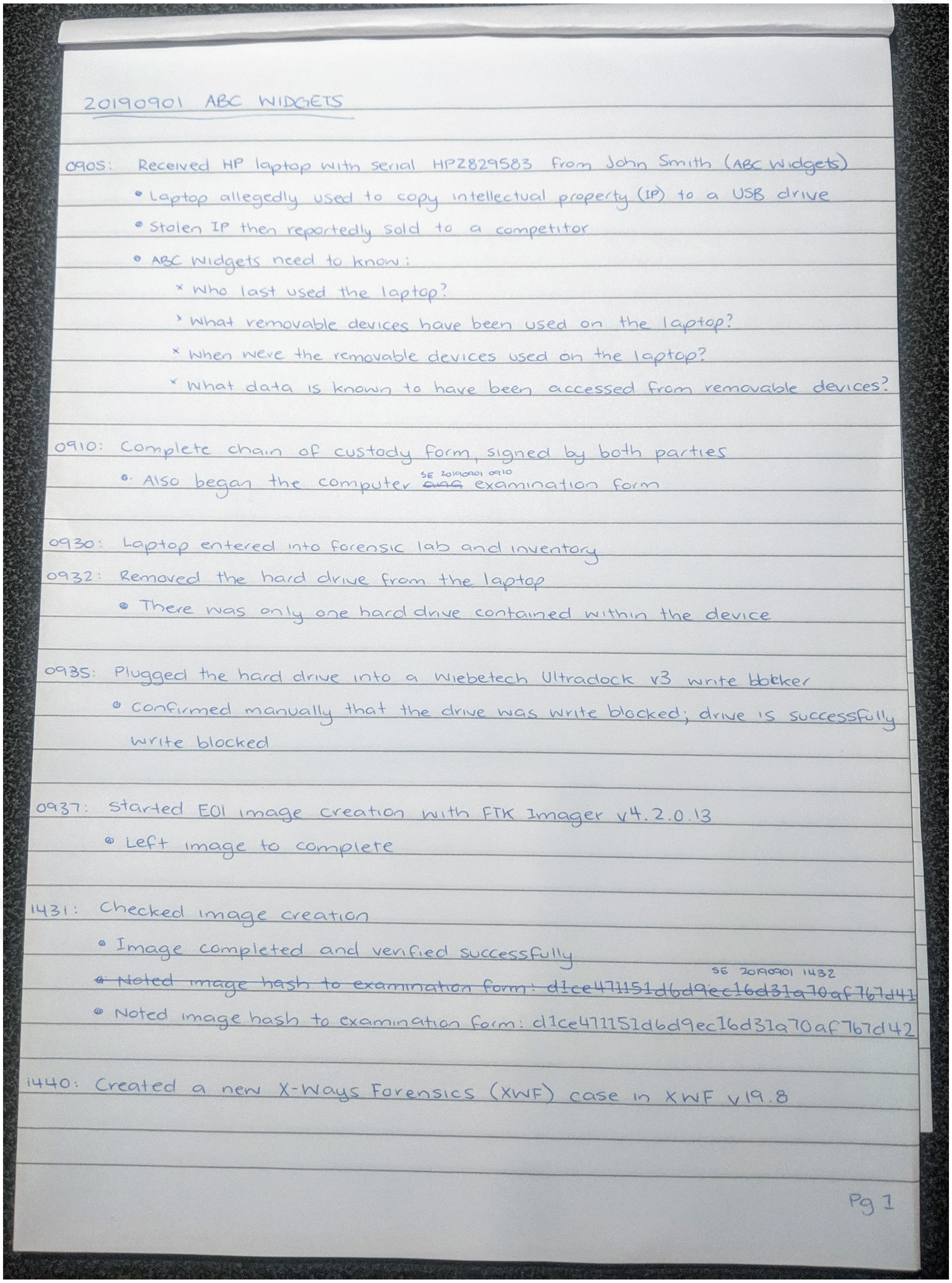
1440: Created a new X-Ways Forensics (XWF) case in XWF v19.8

...

Figure 2: Note Alteration Audit Trail in Confluence

D. Example: Contemporaneous Notes (Physical, Brief)

This Appendix mirrors Appendix C, but in physical form. Note the initials and timestamp for the updated hash (which was written incorrectly in the first instance), and the other correction.



20190901 ABC WIDGETS

0905: Received HP laptop with serial HPZ829583 from John Smith (ABC Widgets)
- Laptop allegedly used to copy intellectual property (IP) to a USB drive
- Stolen IP then reportedly sold to a competitor
- ABC Widgets need to know:
  - × Who last used the laptop?
  - × What removable devices have been used on the laptop?
  - × When were the removable devices used on the laptop?
  - × What data is known to have been accessed from removable devices?

0910: Complete chain of custody form, signed by both parties
- Also began the computer SE 20190901 0910 ~~and~~ examination form

0930: Laptop entered into forensic lab and inventory
0932: Removed the hard drive from the laptop
- There was only one hard drive contained within the device

0935: Plugged the hard drive into a Wiebetech Ultradock v3 write blocker
- Confirmed manually that the drive was write blocked; drive is successfully write blocked

0937: Started E01 image creation with FTK Imager v4.2.0.13
- Left image to complete

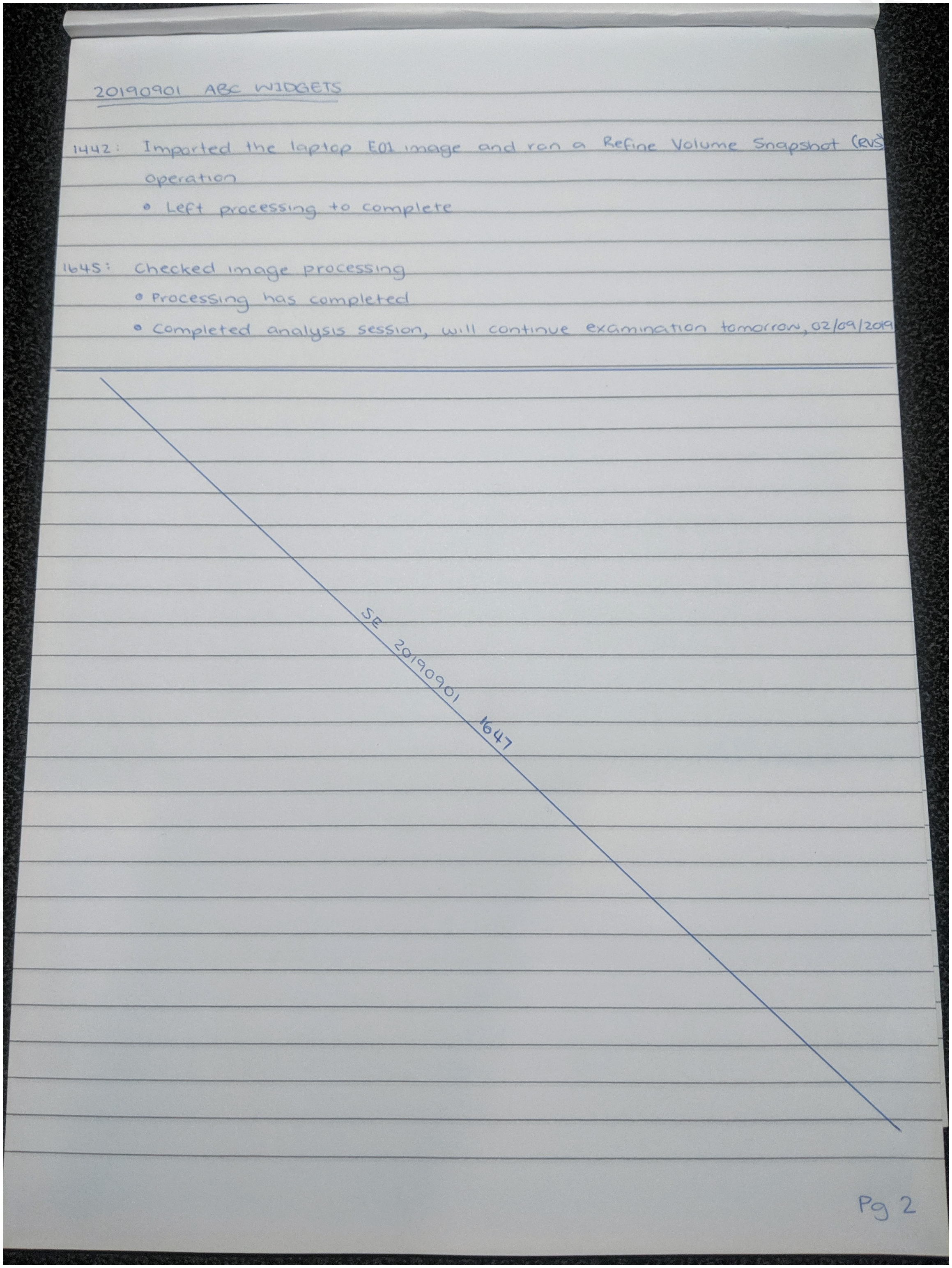
1431: Checked image creation
- Image completed and verified successfully
- SE 20190901 1432 ~~Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d41~~
- Noted image hash to examination form: d1ce471151d6d9ec16d31a70af767d42

1440: Created a new X-Ways Forensics (XWF) case in XWF v19.8

Pg 1

Figure 3: Physical Contemporaneous Notes

Below are the continued notes from above, with a strike through the unused portion of the page to make clear later additions which don't belong.



20190901 ABC WIDGETS

1442: Imported the laptop E01 image and ran a Refine Volume Snapshot (RVS operation

- Left processing to complete

1645: Checked image processing

- Processing has completed
- Completed analysis session, will continue examination tomorrow, 02/09/2019

SE 20190901 1647

Pg 2

Figure 4: Physical Contemporaneous Notes