applied sciences

MDPI

Article

Forensic Exchange Analysis of Contact Artifacts on Data Hiding Timestamps

Da-Yu Kao

Department of Information Management, Central Police University, Taoyuan City 33304, Taiwan; camel@mail.cpu.edu.tw

Received: 1 May 2020; Accepted: 3 July 2020; Published: 7 July 2020

Abstract: When computer systems are increasingly important for our daily activities, cybercrime has created challenges for the criminal justice system. Data can be hidden in ADS (Alternate Data Stream) without hindering performance. This feature has been exploited by malware authors, criminals, terrorists, and intelligence agents to erase, tamper, or conceal secrets. However, ADS problems are much ignored in digital forensics. Rare researches illustrated the contact artifacts of ADS timestamps. This paper performs a sequence of experiments from an inherited variety and provides an in-depth overview of timestamp transfer on data hiding operations. It utilizes files or folders as original media and uses the timestamp rules as an investigative approach for the forensic exchange analysis of file sets. This paper also explores timestamp rules using case examples, which allow practical applications of crime scene reconstruction to real-world contexts. The experiment results demonstrate the effectiveness of temporal attributes, help digital forensic practitioners to uncover hidden relations, and trace the contact artifacts among crime scenes, victims, and suspects/criminals.

Keywords: data hiding; temporal attributes; timestamp transfer; exchange principle; trace evidence; contact artifacts; crime scene reconstruction; cybercrime investigation; digital forensics

1. Introduction

Timestamps in the reconstruction of cybercrimes have proven to be an expedient source of evidence for digital forensic practitioners [1]. Active malware or criminals have implemented antiforensic techniques to hide their traces. When practitioners conduct a crime scene reconstruction, it is essential to identify user data hiding activity [2]. Practitioners that have a good understanding of timestamp transfer and data hiding techniques will be better equipped to collect and acquire digital evidence in line with the legal requirements for prosecuting criminals. As file metadata may reveal the trace evidence of contact artifacts, there is critical information hidden in the file systems. However, the existing research regarding timestamp rule analysis does not consider the contact artifacts and data hiding [1,3–5]. ADS (Alternate Data Stream) has been exploited by malware authors, criminals, terrorists, and intelligence agents to erase, tamper, or conceal secrets [6]. This paper focuses on the forensic exchange analysis of the NTFS (New Technology File System) and examines the ADS cover media under different user behaviors. The challenge of these ADS operations lies in the hidden data, which are not readily visible using the File Explore application program in Windows [7]. Forensic exchange analyses have shed light on the causes and correlations of digital data or event records [8]. The values of various temporal attributes can be examined to explore the intricate user behavioral activities or hidden facts. If criminals create, archive, or copy a file into a folder, it updates the specific temporal value and reveals the truth of a crime [9]. The collection of timestamps enables practitioners to review chronological activity in a cybercrime investigation. A practical problem may arise when a criminal hide ADS files on purpose in a cybercrime case. Can we find any timestamp rules in ADS cover media? If practitioners cannot analyze hidden files properly, then the investigation could be affected.

It is thus very critical that practitioners are highly sensitive to exploring any user timestamp behaviors. This paper considers the forensic exchange analysis task: This context performs ADS operations and discovers their timestamp rules. The researcher tests this by using two controlled experiments [10]:

- A discovery experiment (Section 3.3) to repeatedly classify temporal attributes as timestamp rules.
- An ADS experiment analogous to Kao and Chan in 2017 [11] as conducting comparative analyses in Case 2 (Section 5.2).

Practitioners with knowledge and expertise play an unquestionably critical role in identifying divisible evidence and collecting any temporal attributes from the crime scene [12]. The existence of trace evidence is not unique to physical evidence. Linking the digital evidence of contact artifacts is critical to discover other connected devices [13]. This paper aims to address short-term changes in ADS behavioral relationships by performing a temporal dissection of classification. It provides a first step towards uncovering hidden behavioral changes via temporal dissection of contact artifacts [14]. The uniqueness and contributions of this paper are listed below:

- Perform a sequence of experiments to explore the contact artifacts of timestamp transfer.
- Analyze temporal attributes and propose some timestamp rules from ADS operations.
- Uncover hidden relations using timestamp rules from an inherited variety.
- Support practitioners to explore any possible contact artifacts in connected devices.
- Evaluate the efficacy of several temporal values to reconstruct an event.
- Provide an in-depth overview of timestamp transfer on data hiding operations from a forensic exchange analysis perspective.

This paper is organized as follows. In Section 2, background information is given that shall help to understand the forensic exchange analysis on data hiding timestamps. The divisible matters in temporal attributes give insights into the contact artifacts of ADS operations. The experimental environment, forensic process plan, and observation scenario are presented in Section 3. Section 4 describes the proposed timestamp rules from the following viewpoints: direct analysis on original media (temporal reconstruction), cross-sectional analysis of timestamp orders (relational reconstruction), ADS operation analysis on cover media (functional reconstruction), and analysis results of file sets. The forensic exchange analysis of two case samples is illustrated in Section 5. The conclusions are given in Section 6.

2. Background

Most practitioners have been asked whether they can prove a suspect was at the keyboard at a specific time. Without corroborating evidence from various objects or sources, it is virtually difficult to collect the multiple versions of the truth or place a person at the keyboard [15]. Edmond Locard's exchange principle states that every contact leaves a trace among crime scenes, victims, and suspects/criminals [16]. Whenever two objects come in contact, a timestamp transfer of divisible material occurs. There will be an exchange between two objects. When criminals enter and subsequently depart a crime scene, they will leave something behind and take something with them [17]. The contact artifacts in servers or client computers can serve as the digital equivalent to DNA, hair, fibers, and trace evidence [1,17]. These data may provide primary sources of information to reconstruct events between suspects and victims at a crime scene [18]. There is an increasing need for practitioners to find divisible temporal attributes and to link the timestamp transfer of connected devices at a crime scene. This exchange principle of forensic science can apply to digital material in analyzing data hiding timestamps. Background information is presented in this section.

2.1. Divisible Temporal Attributes of ADS Contact Artifacts

The data stream default for an NTFS file is an unnamed $DATA attribute, which contains the standard file content. When a file has more than one $DATA attribute, the additional attributes are sometimes referred to as ADS. ADS can hide data as any format in additional $DATA attributes, which must have names and can be allocated to an MFT (Master File Table) entry. Windows $MFT stores metadata about the files and includes internal management data. The method of creating and managing these metadata can vary according to the different operations on a system [1]. When a file is processed, these time values are identical, but their contents are somewhat different [18]. The temporal attributes of $SI ($STANDARD_INFORMATION) and the $FN ($FILE_NAME) hold the following four forensically impressive values in Table 1 [18,19]: INDX Entry/Filename date changed time, modified time, accessed time, and created time. Table 1 illustrates and synchronizes the timestamp terminology used by the NTFS file system. Timestamps can be recorded in a different circumstance when certain events occurred recently. Windows stores data content in $DATA attributes and keeps $SI/$FN temporal attributes [19].

Table 1. Timestamp terminology.

Temporal Attributes		Properties in FTK	
EMAC-time	$SI (STANDARD_INFORMATION)	$SI.E-time	INDX Entry Date Changed
		$SI.M-time	INDX Entry Date Modified
		$SI.A-time	INDX Entry Date Accessed
		$SI.C-time	INDX Entry Date Created
	$FN ($FILE_NAME)	$FN.E-time	Filename Date Changed (MFT)
		$FN.M-time	Filename Date Modified (MFT)
		$FN.A-time	Filename Date Accessed (MFT)
		$FN.C-time	Filename Date Created (MFT)

In 2017, we had demonstrated various methods to hide data in ADS and discussed its implications for digital forensic investigation [20]. That paper has shown the locations where criminals can create ADS and where the practitioner can find hidden information. The experimental output includes the file name, timestamp, and file size. For example, the task manager of the file system can detect the name of the ADS file. The update of timestamps can show abnormal signs for ADS behaviors. The file size of cover media can be detected. Most antivirus programs do not scan Windows ADS for viruses, trojans, and other malicious codes [21]. Malware such as TeslaCrypt ransomware can be associated with a malicious ADS file to bypass detection or infect a target system [2]. It can be accessed with the echo, notepad, or type commands. In Table 2, some ADS detection techniques, such as LADS, Streams, AlternateStreamView, and DOS DIR/r commands, are often discussed to detect stealth ADS files [9,22].

Nevertheless, these tools show a few temporal attributes. ADS still leaves behind its detectable trace. Our previous research findings in 2017 are illustrated as follows [20].

- Different detection methods can identify various ADS items and present consistent content.
- DOS DIR/r command and AlternateStreamView can detect more complete ADS data than others.
- The stream size of original media remains the same and bypass detection.
- Its stream allocated size increases in the results of the AlternateStreamView program.

Even though a hidden ADS file is attached intentionally or systematically, it remains in the storage space. The existing ADS detection tools could be applied to the Windows NTFS file system so that the performance and accuracy of observational experiments could also be evaluated to detect temporal attributes to fight against cybercrime. In Table 3, the matrix rows systematically review the similarities and differences among these techniques, and the columns are the toolkit dimensions for the comparison. Some third-party tools can explore cybercrime artifacts and view ADSs [22], including a Windows function (DOS DIR/r command), LADS (available from heysoft.de), Streams (available from microsoft.com), AlternateStreamView (available from nirsoft.net), and FTK (available from accessdata.com). The native Windows function of the DIR command displays all read-only information about files, directories, name, size, available disk space, and last modification time in the current directory. The /r option can show any ADS and is always suffixed with $DATA. These third-party ADS detection tools are designed for detecting these hidden files within the ADSs. LADS can locate data in ADS on a system. Streams can examine the files/directories and inform users of the name and sizes of any named streams it encounters within those files. AlternateStreamView can scan, find, view, copy, or delete all hidden ADS in the NTFS drive. In FTK, practitioners can hit the properties tab in the view pane, view the NTFS timestamps in the file metadata, and understand what happened to a file. Any of these tools can examine the files and directories of any ADSs, which are specific to these NTFS artifacts. Forensic toolkits can provide many chances to extract traces from multiple temporal attributes and explore the timestamp transfer of trace evidence in relevant systems. With the right tools, it becomes useful to determine if digital evidence has been modified or tampered with by comparing them with other sources.

Table 2. Popular ADS (Alternate Data Stream) techniques.

Type	Tools	Statement	Sample
Creation	Echo	Add data to ADS	echo “This is another ADS test file”> test.txt:ads.txt
	Type or copy		type marked.exe > test.txt:ads.exe copy marked.exe > test.txt:ads.exe
	>		marked.txt > original.txt:malicious.txt
List	DIR /r	Lists the ADS files	dir/r
	LADS		
	Streams		
	AlternateStreamView		
Access, modification or overwriting	Notepad	Open, modify, or overwrite ADS text file	notepad test.txt:ads.txt
	MSPaint	Open, modify or overwrite images and graphics	mspaint test.txt:ads.jpg
	Start	Execute PE file (Disable after Windows Vista version)	start test.txt:ads.exe
Deletion	Echo	Remove ADS file	echo “deleted ADS” > test.txt:ads.exe

Table 3. Comparative analyses in detecting ADS operations.

Analyses	Techniques		
	Native	Third-Party	
	DOS DIR/r Command	LADS, Streams, AlternateStreamView	FTK
Differences	A Windows function	ADS detection tools	Forensic toolkit
Similarities	All techniques can find and retrieve ADS information in NTFS artifacts		

2.2. Timestamp Transfer on Linking the Connected Devices

The timestamp rules in NTFS are very complicated and are dependent on both file types and ADS operations [3]. How NTFS sets or updates timestamps depends on the type of lower-level file operations. It involves multiple interactions among the shells, NTFS, applications, and various configurations or settings in Windows [23]. Moreover, the SetFileTime function can modify timestamps without changing the file content. The SystemTimeToFileTime function can convert a timestamp to specified file time [24]. Windows API function calls in various configurations or versions will strongly impact how NTFS timestamps are created or updated. Microsoft has documented both NTFS behavior and Windows APIs for various versions [25].

Cybercrime creates a negative impact on societies and creates potential risks for the economy [26]. A digital action taken by a criminal will leave traces of that activity on the system. A timestamp is correctly reflected when something occurs [24]. Even simple operations such as copy and move may be very complicated to change metadata or create artifacts to the system [27]. Viewing the timestamps in an event through the transfer of Locard's exchange principle can be very helpful in detecting and analyzing these contact artifacts, not only physical but also digital evidence [8]. Timestamps show the time status of a particular digital file. In 2008, Willassen proposed to create a system model by listing possible action sequences and their timestamp orders [5]. In 2011, Bang, Yoo, and Lee analyzed the change in temporal attributes with file operations [3]. In 2020, Palmbach and Breitinger examined the reliability of artifacts to detect timestamp operations in the NTFS file system [1]. Capturing some contact artifacts in multiple interactions can help practitioners collect digital evidence effectively and generate interesting insights, which lead to a better understanding of criminal behavior [28]. It is possible to link the timestamp transfer to former operations, correlate behavior activities, and identify a suspect during a digital investigation [29].

While many studies are present for identifying the source digital device of cover media [7,22,30,31], a little progress has been made for crime scene reconstruction of hidden files. The timestamp order of files is utilized to trace the timeline of relevant events [32]. Although some papers have discussed timestamp evaluation, they do not analyze data hiding operations [1,3–5,27]. Using a variety of forensic tools and techniques can provide timeline analysis of file metadata, which can help practitioners reason about how trace evidence of different types are logically connected and how they fit together in the big picture of a case [13]. It can produce a summary narrative of forensic exchange analysis in data hiding activities. Therefore, this paper tries to present an experimental method to analyze temporal attributes and identify the trace evidence of former ADS operations.

3. Research Design

The researcher is interested in the timestamp transfer of contact artifacts, which are based on ADS operations. A second aspect is to explore what kind of relevant digital evidence can be deduced and inferred from the forensic process plan in Figure 1 [29]. Analysis tasks are performed in an observation scenario to describe the timestamp transfer of contact artifacts when these ADS detection tools can find and retrieve stealth ADS information for diverse investigative needs. In order to improve the detection of these emerging data hiding techniques, this paper aims to answer the following three RQs (Research Questions) [1,22]:

- RQ 1. Are there any timestamp rules from temporal values in ADS operations?
- RQ 2. Can a practitioner uncover hidden relations in an inherited variety?
- RQ 3. Can a practitioner trace the contact artifacts of cover media?

3.1. Experimental Environment

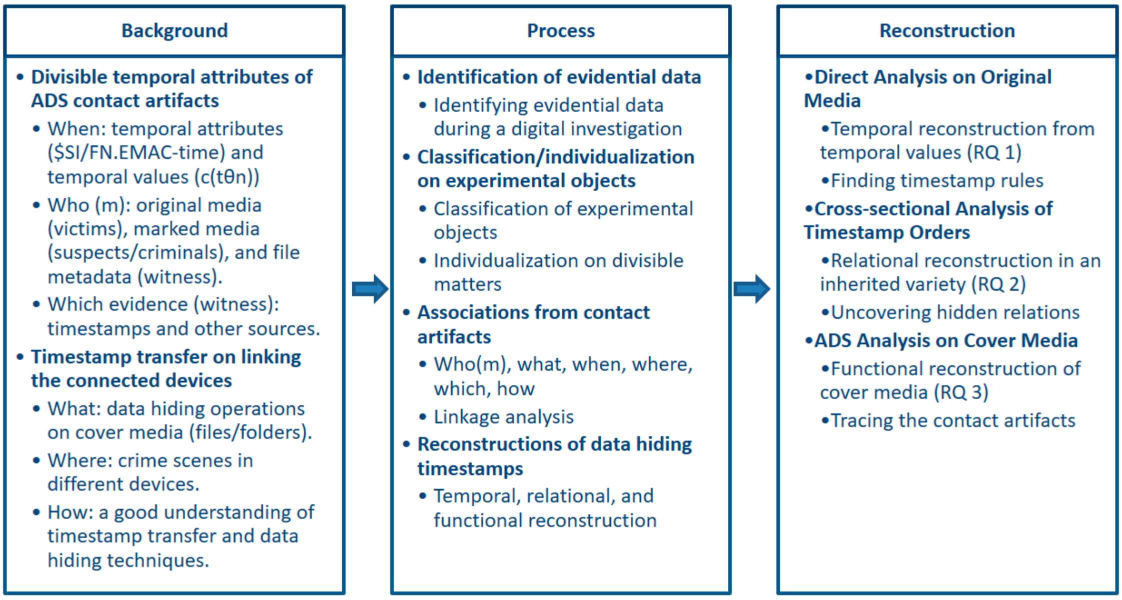
Practitioners are still facing the challenge of a shortage of knowledge on how ADS timestamps are updated with different file operations. Besides, there is no systematic documentation on the timestamp rules. This experiment utilizes files or folders as original media and uses the timestamp rules as an investigative approach for NTFS file systems [33]. The forensic FTK tool can retrieve the temporal value of cover media, discover contact artifacts, and offer more temporal value than other ADS detection tools. The file sizes in this experiment are less than 1 MB. The experimental environment is illustrated in Table 4.

3.2. Forensic Process Plan

Cybercrimes continue to emerge. Advancements in modern technology have enabled them to commit a diverse range of criminal activities [34]. Practitioners should be aware of how suspects and victims interact with each other at digital crime scenes. Some fundamental questions of digital evidence that need to be addressed during a cybercrime investigation are what is it (identification), what characteristics distinguish it (classification or individualization), how the strength of transfer evidence should be determined (association), and what kind of evidence can understand the sequence of past events (reconstruction) [16]. The forensic process plan of timestamp transfer in Figure 1 includes identification of evidential data, classification/individualization of experimental objects, associations from contact artifacts, and crime scene reconstructions of data hiding timestamps. This plan tries to identify any trace evidence in contact artifacts and explores how ADS affects the timestamps of cover media.

Table 4. Experimental environment.

		Tool	
Type	**Details**	**Application Name**	**Details**
OS	Windows 7 Ultimate, 64-bit	Edit	Microsoft Office Word Notepad
File system	NTFS file system	Forensic Toolkit	AccessData FTK Toolkit 6.2.1 AccessData FTK Imager 3.4.2.6.
Drive	F and G	ADS Detection	AlternateStreamView v1.53, 64-bit
Experimental objects	Folder, Text, and Word	Visual Analysis	IBM i2 Analyst's Notebook v8.9



Background

- **Divisible temporal attributes of ADS contact artifacts**
  - When: temporal attributes ($SI/FN.EMAC-time) and temporal values (c(tθn))
  - Who (m): original media (victims), marked media (suspects/criminals), and file metadata (witness).
  - Which evidence (witness): timestamps and other sources.
- **Timestamp transfer on linking the connected devices**
  - What: data hiding operations on cover media (files/folders).
  - Where: crime scenes in different devices.
  - How: a good understanding of timestamp transfer and data hiding techniques.

Process

- **Identification of evidential data**
  - Identifying evidential data during a digital investigation
- **Classification/individualization on experimental objects**
  - Classification of experimental objects
  - Individualization on divisible matters
- **Associations from contact artifacts**
  - Who(m), what, when, where, which, how
  - Linkage analysis
- **Reconstructions of data hiding timestamps**
  - Temporal, relational, and functional reconstruction

Reconstruction

- **Direct Analysis on Original Media**
  - Temporal reconstruction from temporal values (RQ 1)
  - Finding timestamp rules
- **Cross-sectional Analysis of Timestamp Orders**
  - Relational reconstruction in an inherited variety (RQ 2)
  - Uncovering hidden relations
- **ADS Analysis on Cover Media**
  - Functional reconstruction of cover media (RQ 3)
  - Tracing the contact artifacts

Figure 1. Forensic process plan of timestamp transfer.

(1) Identification of evidential data

The identification of evidential data focuses on identifying the digital evidence of criminal activities and collecting the trace evidence of former data hiding operations. When a file is associated with crimes, the temporal attributes of the file plays a vital role in digital forensics. $SI attribute manages the temporal attributes. The $SI.E-time is hidden from users. Various temporal attributes obtained from file property is only the \$SI.MAC-time. \$SI.EMAC-time is updated when a file is accessed or operated. The \$FN attribute of timestamps is more stable than \$SI. Windows do not often update \$FN temporal values when \$SI attributes are much sensitive to diverse processes [11,18]. Windows do not typically update the \$FN.EMAC-time. These values are updated only when the file is created, renamed, or moved for name management. Every file has a \$DATA attribute, which contains the content and takes care of data management.

(2) Classification/individualization of experimental objects

The experimental objects are discussed in two parts: classification/individualization. The classification of experimental objects (folder, text, and Word) helps the researcher explore their temporal values and timestamp rules. The method to create ADS in a file or folder is similar to each other. The individualization on divisible matters is presented as temporal attributes (\$SI/FN.EMAC-time) in this paper. The researcher can list the timestamp sequences and determine if the observed result is consistent.

(3) Associations from contact artifacts

Temporal attributes will be updated while users apply ADS to hide information. Practitioners can interpret temporal attributes and extract relevant temporal value from file metadata without interfering with the data. While they have an opportunity to examine a digital crime scene in its original state, the temporal value of evidence dynamics can provide some clues to examine the relevant files on evidential devices [18]. Practitioners can try to explore this possibility to acquire the contact artifacts of executed operations and find any available linkage relationship.

(4) Reconstructions of data hiding timestamps

Crime scene reconstruction is the most crucial step of any forensic investigation of a possible criminal act [18]. It establishes what occurred and analyzes the evidence and circumstances of a crime at the scene. It also focuses on recognizing the potential evidence, gathering as much data and evidence to form a valid argument, and gaining a complete understanding of a crime. ADS operations can transfer some trivial temporal value in various contact artifacts. Combined with the information from other sources, practitioners can have greater confidence in reconstructing crime scenes. Temporal attributes are taken into account to see if a device was used to provide an answer to a question during a specific period in time. These timestamp rules can help practitioners discover ADS trace evidence to a digital environment. The crime scene reconstructions of data hiding timestamps are illustrated from:

- Temporal reconstruction to establish an event timeline,
- Functional reconstruction to uncover secret messages of former data hiding operations, and
- Relational reconstruction to correlate behavioral activities among crime scenes, victims, and suspects/criminals.

3.3. Observation Scenario

This experiment adopts the iterative steps in Appendices A–C to collect data from 23 June to 9 August 2019 and explore timestamp rules. The time zone is UTC (Coordinated Universal Time) for FTK 6.2.1 records. The observation formulates a scenario on experimental objects (cover media). Steganography is the process of hiding confidential data on cover media, which can be divided into two parts [30]: original media and marked media. Original media are visible in Windows Explorer or via the "dir" command such as "F:\F1," "F:\T1.txt," and "F:\W1.doc." Marked media, the output of the embedding module, is perceptually identical to original media but with data hidden. In this paper, it is the ADS itself, such as "F:\F1:EF-1.txt\," "F:\T1.txt:ET-1.txt," and "F:\W1.doc:EW-1.txt." Based on the ADS commands in Table 5, the inherited variety of cover media is illustrated as $\boldsymbol{A}$–$\boldsymbol{A}^4$ and $\boldsymbol{B}$–$\boldsymbol{B}^3$.

All timestamps are recorded and identified in three stages. The observation scenario was designed to find whether there are any timestamp rules in ADS operations. A timestamp order is a logical series of all elements in the stamping time set θ, where each element is related to the next one in the sequence with the approximately equal relation "≒," the equal relation "=," or the less-than relation "<." The approximately equal relation is anything that is intentionally similar but not exactly equal to something else. The equal relation implies that these timestamps were set at the same time. The less-than relation implies that the first timestamp is earlier than the second. Each object has n different timestamps θ1, θ2, . . . , θn. Sequential timestamps also record each step, where n is set to "27" in this experiment. The updated timestamps are underlined for comparison in Tables 6–8. These timestamps were set in time tθ1, tθ2, ..., tθn, where the temporal values observed by the researcher are c(tθ1), c(tθ2), ..., c(tθn) [4]. These experimental processes are documented to be repeated or conducted by the practitioner or a third party for obtaining comparable results and evolving the expected findings.

In Stage 1 (creation), the researcher first explores the timestamps as the baseline data and gathers its temporal attributes to identify their initial status. The basic notation of an ADS file is <filename>:<ADSname>. In Table 6, Stage 1(a) and 1(c) is the file creation on original media. Stage 1(b) and 1(d) are the 1st ADS creation on marked media. Stage 1(e) is the 2nd ADS creation on marked media. $SI and $FN-time of original media are created in Stage 1(a)(c). Stage 1(e) updates $SI.M-time of 1st ADS marked media, which is no content change. It shows the contact artifacts between two marked media in 2nd ADS creation. $SI.AC-time of marked media is inherited from the original media in Stage 1(b)(d)(e). It shows the contact artifacts in ADS creation operations. Table 6 illustrates the contact artifacts in ADS creation operations and indicates the hidden relations among the following inherited varieties: $\boldsymbol{A}$ and $\boldsymbol{A}^{\mathbf{1}}$ in Stage 1(a)(b), $\boldsymbol{B}$ and $\boldsymbol{B}^{\mathbf{1}}$ in Stage 1(c)(d), and $\boldsymbol{A}$ and $\boldsymbol{A}^{\mathbf{2}}$ in Stage 1(a)(e).

In Stage 2 (modification), the researcher investigates the timestamps on original media and 1st ADS modification on marked media in Table 7. Stage 2(a) updates the $SI.M-time of original media and the $SI.MAC-time of its folder. In Stage 2(b), $SI.EM-time of original media and $SI.M-time of marked media are updated. Moreover, $SI.MAC-time and $FN-time of original media are inherited from Step 1–3 and 13–15 in Stage 2(a). A time delay of Step 13–15 occurs in updating the $FN.EM-time of original media. Table 7 illustrates the contact artifacts of relevant timestamps from their former operations and demonstrates the following chances of tracing the contact artifacts: c(tθ1)–c(tθ3) in Stage 1(a) and 2(a) and c(tθ13)–c(tθ15) in Stage 1(e) and 2(a).

In Stage 3 (overwriting), Table 8 illustrates the contact artifacts from multiple operations to uncover hidden relations or trace timestamp transfer. It can provide the great help of digital triage forensics in identifying the connected devices and obtaining actionable intelligence quickly at the scene. Stage 3(a) shows that $SI.MAC-time is inherited from Step 1–3, 11–12, and 18–19. $FN-time of original media is inherited from Step 1–3 and 14–15. In Stage 3(b), $SI.EM-time of original media and $SI.M-time of marked media are also updated and $SI.AC-time of marked media is also inherited from former operations.

Table 5. Experiment setting and ADS observations.

No	Stage	Experiment Setting			Cover Media Observations					
					Original Media		Marked Media			
		ADS Operations	Command	Drive	Without ADS		1st ADS		2nd ADS	
					Time	Variety	Time	Variety	Time	Variety
1	Creation	Open and save	Echo	F	1(a):θ1–3	A	1(b):θ4–6	A^1	1(e):θ13–15	A^2
				G	1(c):θ7–9	B	1(d):θ10–12	B^1	N/A	
2	Modification	Rename and modify	Notepad	F	2(a):θ16–18	A^3	2(b):θ19–21	A^4		
3	Overwriting	Copy and replace	Type	F/G	3(a):θ22–24	B^2	3(b):θ25–27	B^3		

Note: N/A: no information.

Table 6. Functional reconstruction on cover media creation (Stage 1).

Timestamp Rule	Creation Object	Time tθn	Experimental Objects	Temporal Value c(tθn)							
				\$SI [f,g]				\$FN [e]			
				E	M	A	C	E	M	A	C
1(a): F Drive 1st Creation on Original Media (A)											
1	F:\F1	12:52:34 PM(1) 12:52:35 PM(1′) *	Folder [a]	1′	1	1	1	1	1	1	1
4	F:\F1\T1.txt	12:53:45 PM(2)	Folder [d]	2	2	2	1	1	1	1	1
1			Text [a]	2	2	2	2	2	2	2	2
4	F:\F1\W1.docx	12:55:02 PM(3) 12:55:03 PM(3′) * 12:55:04 PM(3″) *	Folder [d]	3″	3″	3″	1	1	1	1	1
1			Word [a]	3′	3′	3′	3	3′	3′	3′	3
1(b): F Drive 1st ADS Creation on Marked Media (A^1)											

Table 6. *Cont.*

Timestamp Rule	**Creation Object**	**Time tθn**	**Experimental Objects**	**Temporal Value c(tθn)**							
				$SI [f,g]				**$FN [e]**			
				E	**M**	**A**	**C**	**E**	**M**	**A**	**C**
1(b): F Drive 1st ADS Creation on Marked Media ($\boldsymbol{A}^{1}$)											
3	F:\F1:EF-1.txt	12:58:00 PM(4)	Folder [c]	4	4	3″	1	1	1	1	1
7			Folder: EF-1.txt [g]	N/A	4	3″	1	N/A			
	F:\F1\T1.txt:ET-1.txt	01:00:36 AM(5)	Folder	4	4	3″	1	1	1	1	1
3			Text [c]	5	5	2	2	2	2	2	2
7			Text: ET-1.txt [g]	N/A	5	2	2	N/A			
	F:\F1\W1.docx:EW-1.txt	01:03:20 AM(6)	Folder	4	4	3″	1	1	1	1	1
3/5			Word [c]	6	6	3′	3	3′[e]	3′ [e]	3′ [e]	3 [e]
7			Word: EW-1.txt [g]	N/A	6	3′	3	N/A			
1(c): G Drive 1st Creation on Original Media (***B***)											
1	G:\F3	01:05:47 AM(7)	Folder [a]	7	7	7	7	7	7	7	7
4	G:\F3\T3.txt	01:06:40 AM(8)	Folder [d]	8	8	8	7	7	7	7	7
1			Text [a]	8	8	8	8	8	8	8	8
4	G:\F3\W3.docx	01:08:06 AM(9) 01:08:07 AM(9′) *	Folder [d]	9′	9′	9′	7	7	7	7	7
1			Word [a]	9	9	9	9	9	9	9	9

Table 6. *Cont.*

Timestamp Rule	Creation Object	Time tθn	Experimental Objects	Temporal Value c(tθn)							
				$SI [f,g]				$FN [e]			
				E	M	A	C	E	M	A	C
1(d): G Drive 1st ADS Creation on Marked Media ($\boldsymbol{B}^{1}$)											
3	G:\F3:EF-1.txt	01:10:54 AM(10)	Folder [c]	10	10	9′	7	7	7	7	7
7			Folder: EF-1.txt [g]	N/A	10	9′	7	N/A			
	G:\F3\T3.txt:ET-1.txt	01:15:07 AM(11)	Folder	10	10	9′	7	7	7	7	7
3			Text [c]	11	11	8	8	8	8	8	8
7			Text: ET-1.txt [g]	N/A	11	8	8	N/A			
	G:\F3\W3.docx:EW-1.txt	01:17:48 AM(12)	Folder	10	10	9′	7	7	7	7	7
3			Word [c]	12	12	9	9	9	9	9	9
7			Word: EW-1.txt [g]	N/A	12	9	9	N/A			
1(e): F Drive 2nd ADS Creation on Marked Media (A^{2})											
3/6	F:\F1:EF-2.txt	01:21:39 AM(13)	Folder[c]	13 [f]	13 [f]	3″ [f]	1 [f]	1	1	1	1
7			Folder:EF-1.txt [g]	N/A	13	3″	1	N/A			
7			Folder:EF-2.txt [g]		13	3″	1				
	F:\F1\T1.txt:ET-2.txt	01:26:02 AM(14)	Folder	13	13	3″	1	1	1	1	1
3/6			Text[c]	14 [f]	14 [f]	2 [f]	2 [f]	2	2	2	2
7			Text:ET-1.txt [g]	N/A	14	2	2	N/A			
7			Text:ET-2.txt [g]		14	2	2				
	F:\F1\W1.docx:EW-2.txt	01:28:21 AM(15)	Folder	13	13	3″	1	1	1	1	1
3/5/6			Word[c]	15 [f]	15 [f]	3′ [f]	3 [f]	3′ [e]	3′ [e]	3′ [e]	3 [e]
7			Word:EW-1.txt [g]	N/A	15	3′	3	N/A			
7			Word:EW-2.txt [g]		15	3′	3				

Note: [a] Rule 1, [c] Rule 3, [d] Rule 4, [e] Rule 5, [f] Rule 6, and [g] Rule 7; N/A: no information; * The rule of time delay in creation operations is that C-time is the most stable value, but $SI.E-time is the most sensitive in this experiment.

Table 7. Functional reconstruction on cover media modification (Stage 2).

Timestamp Rule	Modification Object	Time tθn	Experimental Objects	Temporal Value c(tθn)							
				$SI ^{f,g}				$FN ^{e}			
				E	M	A	C	E ^{e}	M ^{e}	A	C
2(a): F Drive Modification on Original Media (A^3)											
2/5/6	F:\F3	01:30:34 AM(16)	Folder ^{f}	16 ^{b,f}	13 ^{e,f}	3″ ^{f}	1 ^{f}	13 ^{e}	13 ^{e}	3″ ^{e}	1 ^{e}
4	F:\F3\T3.txt	01:32:34 AM(17)	Folder ^{d}	17	17	17	1	13	13	3″	1
2/5/6			Text ^{f}	17 ^{b,f}	14^{e,f}	2 ^{f}	2 ^{f}	14 ^{e}	14 ^{e}	2	2
4	F:\F3\W3.docx	01:35:31 AM(18)	Folder ^{d}	18	18	18	1	13	13	3″	1
2/5/6			Word ^{f}	18 ^{b,f}	15 ^{e,f}	3′ ^{f}	3 ^{f}	15 ^{e}	15 ^{e}	3′	3
2(b): F Drive 1st ADS Modification on Marked Media (A^4)											
3	F:\F3:EF-1.txt	01:43:48 AM(19)	Folder ^{c}	19	19	18	1	13	13	3″	1
7			Folder:EF-1.txt ^{g}	N/A	19 ^{g}	18 ^{g}	1 ^{g}	N/A			
			Folder:EF-2.txt ^{g}		19 ^{g}	18 ^{g}	1 ^{g}				
	F:\F3\T3.txt:ET-1.txt	01:46:41 AM(20)	Folder	19	19	18	1	13	13	3″	1
3			Text ^{c}	20	20	2	2	14	14	2	2
7			Text:ET-1.txt ^{g}	N/A	20	2	2	N/A			
			Text:ET-2.txt ^{g}		20	2	2				
	F:\F3\W3.docx: EW-1.txt	01:49:23 AM (21)	Folder	19	19	18	1	13	13	3″	1
3			Word ^{c}	21	21	3′	3	15	15	3′	3
7			Word:EW-1.txt ^{g}	N/A	21	3′	3	N/A			
			Word:EW-2.txt ^{g}		21	3′	3				

Note: ^{b} Rule 2, ^{c} Rule 3, ^{d} Rule 4,^{e} Rule 5, ^{f} Rule 6, and ^{g} Rule 7; N/A: no information.

Table 8. Functional reconstruction on cover media overwriting (Stage 3).

Timestamp Rule	Overwriting Object	Time tθn	Experimental Objects	Temporal Value c(tθn)							
				$SI				$FN			
				E	M	A	C	E	M	A	C
3(a): F: Overwriting on Original Media ($\boldsymbol{B}^2$)											
	G:\F3 overwrite F:\F3	01:51:42 AM(22)	Folder	19	19	18	1	13	13	$3''$	1
2			Text [b]	22	11	2	2	14	14	2	2
			Word [b]	22	12	$3'$	3	15	15	$3'$	3
	G:\F3\T3.txt overwrite F:\F3\T3.txt	01:57:00 AM(23)	Folder	19	19	18	1	13	13	$3''$	1
2			Text [b]	23	11	2	2	14	14	2	2
	G:\F3\W3.docx overwrite F:\F3\W3.docx	01:58:42 AM(24)	Folder	19	19	18	1	13	13	$3''$	1
2			Word [b]	24	12	$3'$	3	15	15	$3'$	3
3(b): F: 1st ADS Overwriting on Marked Media ($\boldsymbol{B}^3$)											
3	F:\F3:EF-1.txt	02:07:53 AM(25)	Folder [c]	25	25	18	1	13	13	$3''$	1
7			Folder:EF-1.txt [g]	N/A	25	18	1	N/A			
			Folder:EF-2.txt [g]		25	18	1				
	F:\F3\T3.txt:ET-1.txt	02:11:03 AM(26)	Folder	25	25	18	1	13	13	$3''$	1
3			Text [c]	26	26	2	2	14	14	2	2
7			Text:ET-1.txt [g]	N/A	26	2	2	N/A			
			Text:ET-2.txt *	N/A							
	F:\F3\W3.docx: EW-1.txt	03:06:31 AM(27)	Folder	25	25	18	1	13	13	$3''$	1
3			Word [c]	27	27	$3'$	3	15	15	$3'$	3
7			Word:EW-1.txt [g]	N/A	27	$3'$	3	N/A			
			Word:EW-2.txt *	N/A							

Note: [b] Rule 2, [c] Rule 3, and [g] Rule 7; N/A: no information; * The 2nd ADS file of the overwritten object is deleted if there is only 1st ADS file in the source.

4. Experimental Analysis Results

Reconstruction provides data for putting the temporal, relational, and functional pieces of a situation together to reach an understanding of a sequence of past events [16]. For a better understanding of timestamp attributes, the experiment results made a comparison on cover media from the following 3 reconstructions and 10 observations in Table 9: direct analysis on original media (temporal reconstruction), cross-sectional analysis of timestamp orders (relational reconstruction), and ADS operation analysis on cover media (functional reconstruction). The temporal attributes of cover media are analyzed and preserved to find their timestamp rules in this section. The result cross-references both the discrepancies and similarities depending on the experimental objects. It is beneficial for practitioners to evaluate an event if a criminal has manipulated ADS to conceal his offense.

Table 9. Reconstructions on timestamp rules.

RQ	Analysis	Reconstruction	Aim	Observation	Rule	Details
1	Direct analysis on original media	Temporal reconstruction from temporal values	Finding timestamp rules	1	1	Created time similarity
				2	2	Updated time in modification/overwriting
				3	3	Updated time inherited from its marked media
				4	4	Updated folder time inherited from its file creation
2	Cross-sectional analysis of timestamp orders	Relational reconstruction in an inherited variety	Uncovering hidden relations	5	5	$FN timestamp order on original media
				6	6	$SI timestamp order on original media
				7	7	$SI timestamp order on marked media
3	ADS analysis on cover media	Functional reconstruction of cover media	Tracing the contact artifacts	8	1/2	Baseline observation without any ADS operations
				9	6	Original media ($SI.E-time) after ADS operations
				10	7	Marked media ($SI.M-time) after ADS operations

4.1. Direct Analysis on Original Media (Temporal Reconstruction)

When cybercriminals create, modify, or overwrite a file with or without ADS, there is a significant change in the timestamps of file metadata. The case-by-case nature in cybercrime investigations is repetitive and worthy to implement appropriate experiments or guarantee error-free digital evidence in data hiding operations. The experimental times of cover media were stamped in each step, which left some contact artifacts for practitioners to trace their various sources. This paper uses inequality to express the (approximately) equal or less-than relation in the temporal values of cover media. The experiment results explore sufficient temporal attributes from user activities, demonstrate the effectiveness of timestamp rules across various types of file operations, and assists in correlating activities from contact artifacts. Putting these experiment results in a chronological timeline helps to look at the list of timestamps and determine the entire history of an experiment concisely. Then, the researcher can connect the virtual dots from the system, establish the continuity of offense, and obtain a complete picture of events. At a scene, temporal attributes help practitioners limit their in-depth investigation of a set of files or events at a particular timeframe [31].

The 1st observation illustrates the created time similarity in Rule 1. When original media are created, all EMAC-time are technically equaled (Rule 1). Namely, $SI and $FN-time are set and created at the same time. C-time is the most stable value, but $SI.E-time is the most sensitive in this experiment. A time delay may happen during the process. In Step 1, the time delay for F:\F1 folder occurs in $SI.E-time. If timestamps are less than 2 s, it is taken for granted that it is the same operation in computer processing. In Step 3, the sequence of time delay for the W1.docx file is as follows: C-time, EMA-time, and the $SI.EMA-time of its folder. Many factors can influence the timestamps, which are created or updated at various times and for various reasons [35]. However, not all file systems can record timestamps in the same manner [17]. For example, the resolution of C-time on FAT is 10 ms, of M-time is 2 s, and of A-time is 1 day. The NTFS file system delays updates to the A-time for a file by up to 1 h [24].

$$\text{\$SI.EMAC-time} \fallingdotseq \text{\$FN.EMAC-time} \tag{Rule 1}$$

The 2nd observation demonstrates the updated time in modification/overwriting in Rule 2. When users modify or overwrite files, the $SI.E-time of the data is updated in Step 16–18 and 22–24.

$$\text{\$FN.EMAC-time and \$SI.MAC-time} \leq \text{\$SI.E-time} \tag{Rule 2}$$

The 3rd observation exhibits the updated time inherited from its marked media in Rule 3. All ADS operations (creation, modification, and overwriting) will update the $SI.EM-time of original media in Step 4–6, 10–15, 19–21, and 25–27.

$$\text{\$FN.EMAC-time and \$SI.AC-time} \leq \text{\$SI.EM-time} \tag{Rule 3}$$

The 4th observation shows the updated folder time inherited from its file creation in Rule 4. Each file is an individual one, and its creation did not update the timestamp of any other data within the same folder. However, when the files are created, the $SI.EMA-time of its folder is also updated in Step 2–3 and 8–9. It means that there may be ADS operations if the $SI.EM-time of original media is updated.

$$\text{\$FN.EMAC-time} = \text{\$SI.C-time} \leq \text{\$SI.EMA-time} \tag{Rule 4}$$

4.2. Cross-Sectional Analysis of Timestamp Orders (Relational Reconstruction)

The cross-sectional analysis of timestamp orders on cover media is illustrated in Figures 2–4, which extracts the following items: crime scenes (temporal attributes), victims (original media), and suspects/criminals (marked media). The timestamp orders of original media (victim data) and marked media (criminal operations) are also established using a temporal correlation in $SI and $FN. That temporal reconstruction can be utilized to find potentially relevant evidence. The contact artifacts of inherited temporal attributes are everywhere in this experiment. The timestamps of cover media will be fully/partially updated due to various operations in Figures 2–4. Although the timestamps in file metadata have different meanings in Table 1, every timestamp will have a story in its unique sequence. The researcher can explore those relevant files that have the same temporal value, either $SI or $FN. That is why, we can find some inherited attributes in Rule 3–4. The event associations from the contact artifacts are further discussed from the following 5W1H analysis [1]:

- Who (m): original media (victims), marked media (suspects/criminals), and temporal attributes in file metadata (witness).
- What: ADS (data hiding) operations on cover media (files/folders) from suspects/criminals.
- When: temporal attributes in file metadata and temporal values in various timestamps.
- Where: crime scenes in different volumes, disks, targets, systems, locations, or devices.
- Which evidence (witness): file metadata, timestamps, Windows event logs, Prefetch files, link files, Registry keys, cookies, history records, and other sources.
- How: a good understanding of timestamp transfer and data hiding techniques.

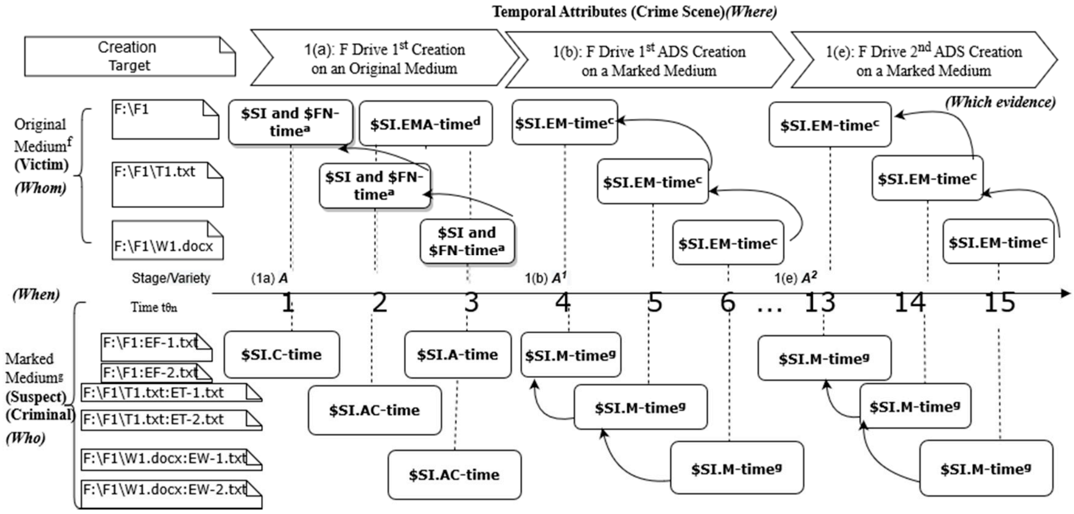


Figure 2. Temporal reconstruction on creation timeline (Stage 1). Note: [a] Rule 1, [c] Rule 3, [d] Rule 4, [f] Rule 6, and [g] Rule 7.

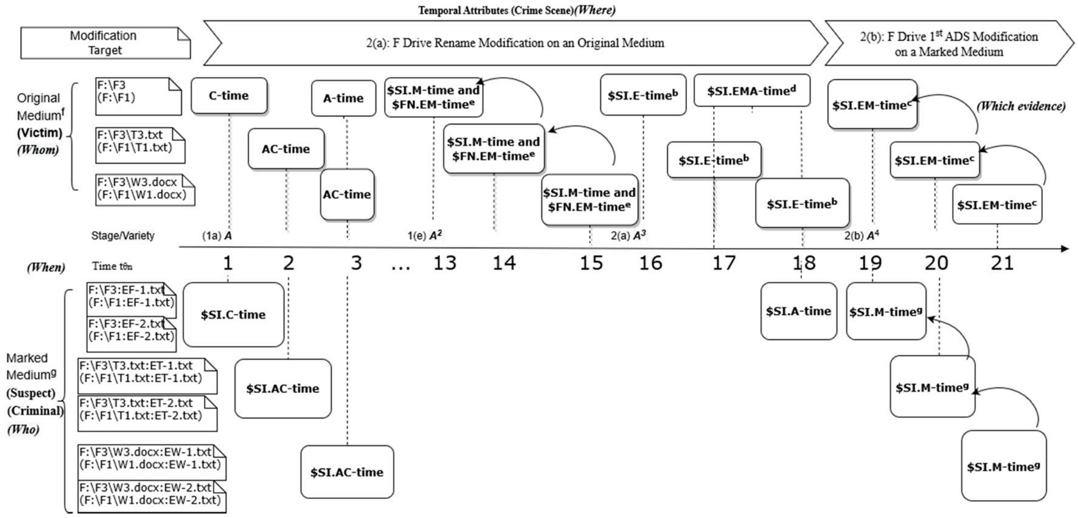

Temporal Attributes (Crime Scene)(Where)
Modification Target
2(a): F Drive Rename Modification on an Original Medium
2(b): F Drive 1st ADS Modification on a Marked Medium
(Which evidence)
Original Medium f (Victim) (Whom)
F:\F3 (F:\F1)
F:\F3\T3.txt (F:\F1\T1.txt)
F:\F3\W3.docx (F:\F1\W1.docx)
C-time
AC-time
A-time
$SI.M-time and $FN.EM-time e
$SI.E-time b
$SI.EMA-time d
$SI.EM-time c
Stage/Variety
(1a) A
1(e) A2
2(a) A3
2(b) A4
(When)
Time tθn
1 2 3 … 13 14 15 16 17 18 19 20 21
$SI.C-time
$SI.AC-time
$SI.A-time
$SI.M-time g
Marked Medium g (Suspect) (Criminal) (Who)
F:\F3:EF-1.txt (F:\F1:EF-1.txt)
F:\F3:EF-2.txt (F:\F1:EF-2.txt)
F:\F3\T3.txt:ET-1.txt (F:\F1\T1.txt:ET-1.txt)
F:\F3\T3.txt:ET-2.txt (F:\F1\T1.txt:ET-2.txt)
F:\F3\W3.docx:EW-1.txt (F:\F1\W1.docx:EW-1.txt)
F:\F3\W3.docx:EW-2.txt (F:\F1\W1.docx:EW-2.txt)

Figure 3. Temporal reconstruction on modification timeline (Stage 2). Note: [b] Rule 2, [c] Rule 3, [d] Rule 4, [e] Rule 5, [f] Rule 6, and [g] Rule 7.

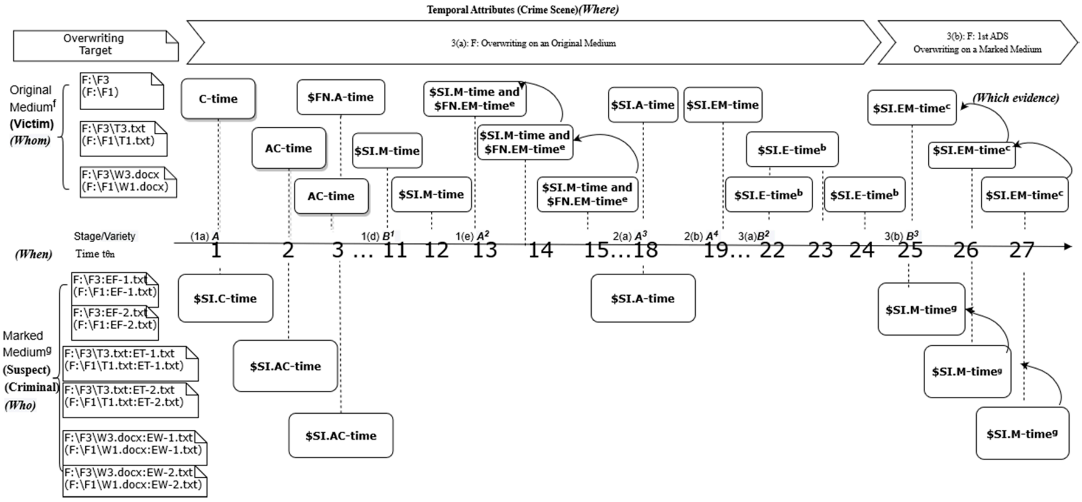

Temporal Attributes (Crime Scene)(Where)
Overwriting Target
3(a): F: Overwriting on an Original Medium
3(b): F: 1st ADS Overwriting on a Marked Medium
(Which evidence)
Original Medium f (Victim) (Whom)
F:\F3 (F:\F1)
F:\F3\T3.txt (F:\F1\T1.txt)
F:\F3\W3.docx (F:\F1\W1.docx)
C-time
AC-time
$FN.A-time
$SI.M-time
$SI.M-time and $FN.EM-time e
$SI.A-time
$SI.EM-time
$SI.E-time b
$SI.EM-time c
Stage/Variety
(1a) A
1(d) B1
1(e) A2
2(a) A3
2(b) A4
3(a)B2
3(b) B3
(When)
Time tθn
1 2 3 … 11 12 13 14 15…18 19… 22 23 24 25 26 27
$SI.C-time
$SI.AC-time
$SI.A-time
$SI.M-time g
Marked Medium g (Suspect) (Criminal) (Who)
F:\F3:EF-1.txt (F:\F1:EF-1.txt)
F:\F3:EF-2.txt (F:\F1:EF-2.txt)
F:\F3\T3.txt:ET-1.txt (F:\F1\T1.txt:ET-1.txt)
F:\F3\T3.txt:ET-2.txt (F:\F1\T1.txt:ET-2.txt)
F:\F3\W3.docx:EW-1.txt (F:\F1\W1.docx:EW-1.txt)
F:\F3\W3.docx:EW-2.txt (F:\F1\W1.docx:EW-2.txt)

Figure 4. Temporal reconstruction on overwriting timeline (Stage 3). Note: [b] Rule 2, [c] Rule 3, [e] Rule 5, [f] Rule 6, and [g] Rule 7.

The 5th observation demonstrates the \$FN timestamp order on original media in Rule 5. \$FN is seldom updated [19]. In this experiment, \$FN.EM-time of original media is inherited from its \$SI.M-time after its 2nd ADS is created on marked media in Step 13–15. The \$FN timestamp order on original media is listed in Rule 5. In creation situations, the \$FN.EMAC-time is set to the values from \$SI.EMAC-time. \$FN.EM-time of original media is updated in Stage 2(a) after its 2nd ADS is created on marked media in Stage 1(e). \$FN.C-time represents the file creation time in the current volume. It is equal to \$SI.C-time in Tables 6–8. In Stage 2(a), a time delay of original media occurs in updating the \$FN.EM-time and \$SI.M-time. Another time delay of updating the folder \$FN.A-time (3″) occurs in Step 16.

$$\$\text{FN.C-time} \le \$\text{FN.A-time} \le \$\text{FN.EM-time} \tag{Rule 5}$$

The 6th observation illustrates the \$SI timestamp order on original media in Rule 6. The \$SI.EMA-time is updated under different scenarios. The \$SI.E-time updates when the MFT entry changes. The \$SI.M-time changes only if the content or metadata are modified. In most pieces of literature, \$SI.A-time is updated while the file is accessed [1,3,12,19,36,37]. However, this experiment does not update \$SI.A-time by default. An exception to this rule is, while text or Word files are renamed, the \$SI.EMA-time of the folder will be updated to the operation time in Stage 2(a). The \$SI.C-time stands for the original creation time in Table 6. It will not be updated by any operations in Tables 7 and 8. In Rule 6, the \$SI.C-time is much more stable than the \$SI.EMA-time.

$$\$\text{SI.C-time} \le \$\text{SI.A-time} \le \$\text{SI.M-time} \le \$\text{SI.E-time} \tag{Rule 6}$$

The 7th observation exhibits the \$SI timestamp order on marked media in Rule 7. In marked media, there is only the \$SI.MAC-time and others are missing values. The \$SI timestamp order on marked media is listed in Rule 7. In Stage 1(b)(d)(e), Stage 2(b), and Stage 3(b), the \$SI.M-time of marked media is often updated to the ADS operation time. The \$SI.A-time of a marked media is inherited from its original media.

$$\$\text{SI.AC-time} \le \$\text{SI.M-time} \tag{Rule 7}$$

4.3. ADS Analysis on Cover Media (Functional Reconstruction)

As a type of file metadata, timestamps can be used to reconstruct events or operations of cover media in a digital investigation. The researcher compares three stages and conducts a relational reconstruction of the collected timestamps to derive the following observations in Tables 8 and 9. Table 10 further observes timestamps from the viewpoint of cover media. The initial letters of filenames for folder, text, and Word are "F," "T," and "W." F drive is the experimental object, and G drive is the data source for comparison and experiment. Table 11 further observes these temporal attributes of timestamp rules. The proposed timestamp rules can be used to promptly identify nearby files of the highest evidentiary value and trace back their related objects by way of the same timestamps in various drives.

Moreover, it will guide practitioners in the right direction to explore the linkage relationship between relevant artifacts and criminal behaviors. The processing time of each step can be observed from the \$SI.E-time (without any ADS operations) or \$SI.EM-time (with ADS operations). If this is true in many cases, then they are reliable. \$SI.M-time of marked media can show the processing time of ADS operations in Rule 7.

Table 10. Relational reconstruction on the timestamp observation of cover media.

Stage/Type	Drive	Cover Media					
		Original Media			Marked Media		
		Folder	Text File	Word File	Folder	Text File	Word File
1(a)1(b)	F:	F:\F1	F:\F1\T1.txt	F:\F1\W1.docx	F:\F1:EF-1.txt	F:\F1\T1.txt:ET-1.txt	F:\F1\W1.docx:EW-1.txt
1(c)1(d)	G:	G:\F3	G:\F3\T3.txt	G:\F3\W3.docx	G:\F3:EF-1.txt	G:\F3\T3.txt:ET-1.txt	G:\F3\W3.txt:EW-1.txt
1(e)	F:	F:\F1	F:\F1\T1.txt	G:\F3\W3.docx	F:\F1:EF-2.txt	F:\F1\T1.txt:ET-2.txt	F:\F1\W1.docx:EW-2.txt
2	F:	F:\F3	F:\F3\T3.txt	F:\F3\W3.docx	F:\F3:EF-1.txt	F:\F3\T3.txt:ET-1.txt	F:\F3\W3.docx:EW-1.txt
3	F:	F:\F3	F:\F3\T3.txt	F:\F3\W3.docx	F:\F3:EF-1.txt	F:\F3\T3.txt:ET-1.txt	F:\F3\W3.docx:EW-1.txt
Creation	$SI $FN	$SI.EMAC-time ≒ $FN.EMAC-time [a]			Missing value for $SI.E-time and $FN.EMAC-time		
Updated Rule	$SI	$SI.E-time [b], $SI.EM-time [c]			$SI.A-time [g]	$SI.M-time[g]	
		$SI.EMA-time [d]	N/A				
	$FN	$FN.A-time [e]	$FN.EM-time [e]		N/A		
Sequential Order	$SI	$SI.C-time ≤ $SI.A-time ≤ $SI.M-time$SI.E-time [f]			$SI.AC-time ≤ $SI.M-time [g]		
	$FN	$FN.C-time ≤ $FN.A-time ≤ $FN.EM-time [e]			N/A		

Note: [a] Rule 1, [b] Rule 2, [c] Rule 3, [d] Rule 4, [e] Rule 5, [f] Rule 6, and [g] Rule 7; N/A: no information.

Table 11. Relational reconstruction among timestamp rules, experimental objects, and their stages.

Observation	**Timestamp Rule**	**Stage**	**1. Creation**	**2. Modification**	**3. Overwriting**
Rule	Cover Media	Experimental Objects	Table 6	Table 7	Table 8
1	Original	File/Folder	≒ [a]	N/A	
2		File	N/A	$SI.E-time [b]	
3		File/Folder	$SI.EM-time [c]		
4		Folder	$SI.EMA-time [d]	N/A	
5		File/Folder	$FN.EM-time [e]	$FN.A-time [e]	N/A
6	Marked		$SI.M-time [g]	$SI.MA-time [g]	
Without ADS operations	Original		EMAC-time [a]	$SI.E-time [b]	
With ADS operations			$SI.EM-time [c]		
	Marked		$SI.M-time [g]		

Note: [a] Rule 1, [b] Rule 2, [c] Rule 3, [d] Rule 4, [e] Rule 5, and [g] Rule 7; N/A: no information.

The 8th observation illustrates the baseline observation without any ADS operations in Rule 1 and 2. Timestamps may produce valuable artifacts of user activities and serve as a valuable source as they record the last time that was performed on a file. A common approach to find related events is to look at the timestamps of the interested cover media. Practitioners can discover the contact artifacts retained behind on the system due to user activities. On original media, the temporal attributes of $SI and $FN in the MFT are similar for a folder, text, and Word creation (Rule 1). In the modification or overwriting of original media, $SI.E-time is updated (Rule 2).

The 9th observation demonstrates the original media ($SI.E-time) after ADS operations in Rule 6. The researcher takes the files and their folder as experimental objects. It applies some operations (create, edit, and overwrite) on them to observe the timestamp variation on cover media. The only telltale sign is that the timestamps of original media may be updated in Rule 1–6. Original media will update $SI.EM-time after its ADS is created, modified, or overwritten. $FN.EMAC-time remains unchanged (Rule 3). When the files are created, the $SI.EMA-time of its folder is also updated (Rule 4). However, $FN.EM-time of original media is updated after its 2nd ADS in Stage 1(e) is created (Rule 5). The $SI.E-time is hidden from users but is also the most sensitive on original media in this experiment (in Rule 6).

The 10th observation exhibits the marked media ($SI.M-time) after ADS operations in Rule 7. When writing to a file, the M-time is not fully updated until all handles for writing are closed [35]. $SI.M-time of marked media can show the processing time of ADS operations in Rule 7. Future additional experiments are necessary to expand these baselines.

4.4. Analysis Results of File Sets

Criminals may use various storage devices for backups. Practitioners will deal with growing numbers of computer devices in a single case. They must adequately select their tools, analyze the data, and detect relevant activities on computer networks with evidence collection in mind [21]. The analysis results of experimental contributions can be further explored from three RQs in this paper.

(1) Temporal reconstruction from temporal values (RQ 1)

Whenever a file/folder is created, modified, or overwritten, a transfer of divisible material always occurs. Every ADS operation can leave the trace of timestamp transfer. Finding timestamp rules from temporal values is critical to explore any possible digital evidence in various devices. For example, the $SI.EMA-time of the folder is updated when a new Word document is created in Step 3 (Table 6). However, the original $SI.C-time and $FN.time of that folder still keeps unchanged at the same time. It is possible to acquire the trace evidence of executed operations and to look for information on external storage devices. Another interesting example is the inherited timestamps of the overwritten file (F:\F3\W3.docx) in Step 24 (Table 8). It demonstrates some contact artifacts of timestamp transfer as follows:

- $SI.E-time: The value of $SI.E-time in Step 24, c(tθ24), shows that the MFT entry record that points to the file is changed in this step.
- $SI.M-time: The value of $SI.M-time in Step 24, c(tθ12), shows that the source file (G:\F3\W3.docx) is modified from Step 12 (Table 6). However, the value of $SI.C-time in Step 12, c(tθ9), shows that its source file (G:\F3\W3.docx) is created from Step 9 (Table 6).
- $SI.C-time and $FN.AC-time: The value of $SI.C-time and $FN.AC-time in Step 24, c(tθ3), shows its very original source file (F:\F1\W1.docx), which is created in Step 3 (Table 6).
- $FN.EM-time: The value of $FN.EM-time in Step 24, c(tθ15), shows that there is a hidden relation with former ADS operation file (F:\F1\W1.docx:EW-2.txt), which is created in Step 15 (Table 6).

(2) Relational reconstruction in an inherited variety (RQ 2)

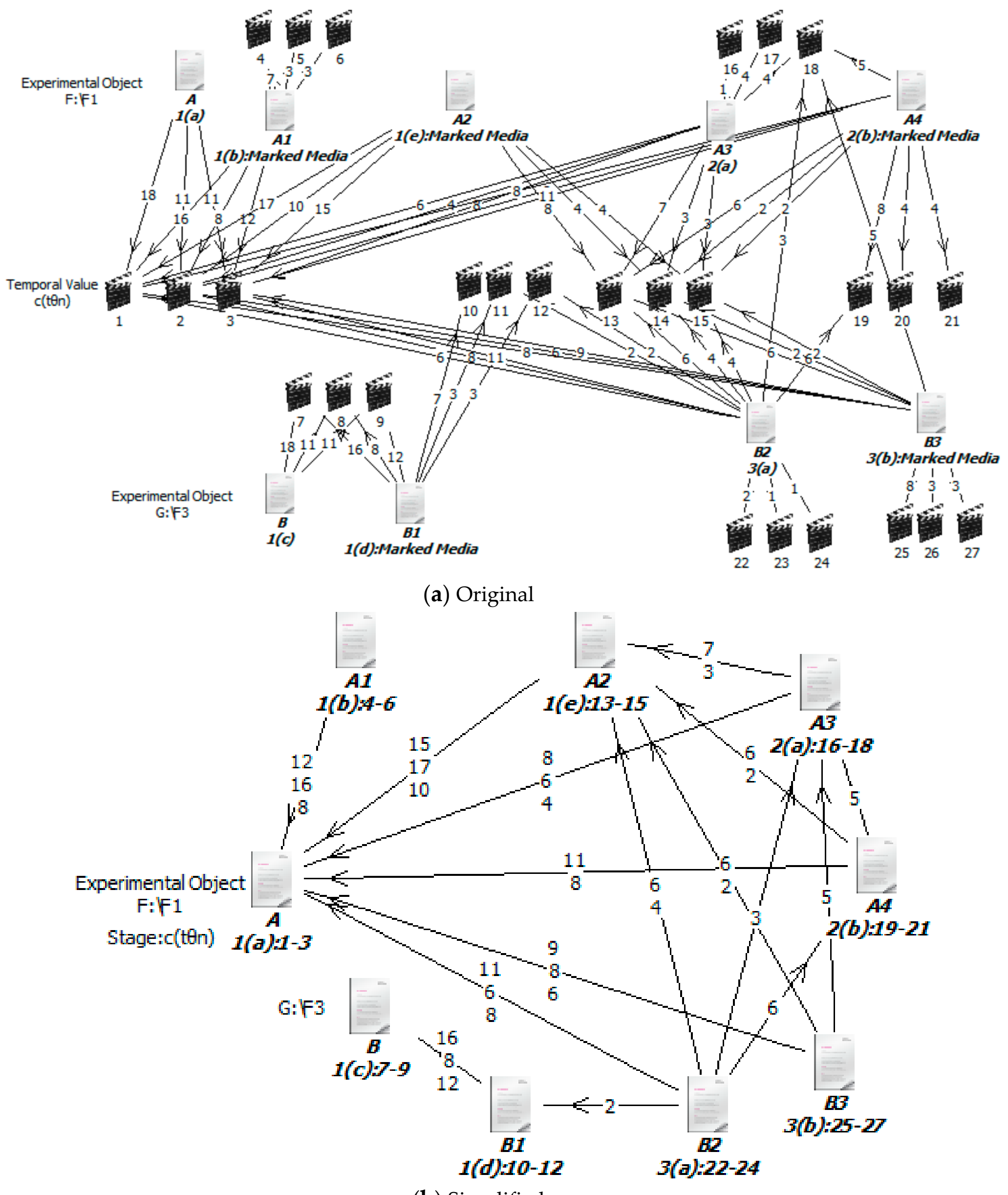
ADS data hiding techniques can hide secret messages in ordinary files. Cover media is often updated as time passes. The criminal can use it to secure his digital files and protect his criminal evidence [11]. When digital data is saved, copied, and used from different locations, it will result in multiple copies at various electronic devices. Hiding activity on an original media is typical for a criminal in several cases where practitioners have to uncover hidden relations in order to obtain evidence. Uncovering hidden relations in an inherited variety is possible in the contact artifacts of cover media from their temporal values. The temporal values in Tables 6–8 also indicate their source and help practitioners trace relevant files in various devices. For example, $\boldsymbol{A^3}$ is inherited from $\boldsymbol{A^2}$ and $\boldsymbol{A}$ when temporal values show c(tθ13)–c(tθ15) and c(tθ1)–c(tθ3) in Stage 2(a). Moreover, $\boldsymbol{A^4}$ is also inherited from $\boldsymbol{A^3}$, $\boldsymbol{A^2}$, and $\boldsymbol{A}$ when the temporal values show c(tθ18), c(tθ13)–c(tθ15), and c(tθ1)–c(tθ3) in Stage 2(b). Even though the content of the variety $\boldsymbol{B^1}$ has been overwritten in Step 24, practitioners still can trace the timestamp transfer among the temporal values c(tθ3), c(tθ9), c(tθ12), c(tθ15), and c(tθ24) to find the relevant files. Their hidden relations in the inherited variety of cover media are also discovered among the sequential variety $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{B^1}$, $\boldsymbol{A^2}$, and $\boldsymbol{B^2}$ in Tables 6–8.

It is very complicated but interesting to link or cross-reference their mutual relationships among these files during an investigation. The researcher uses IBM i2 Analyst's Notebook to analyze the data in Tables 6–8 and discovers the visual contacts in Figure 5, which facilitates the relational reconstruction from temporal values and inherited varieties. Figure 5a illustrates its original status. Figure 5b further merges the related entities to provide an aggregated view of information. Some divisible temporal attributes of contact artifacts happen in Figure 5b:

- $A^{1\text{–}4}$ and $B^{2\text{–}3}$ are inherited from A, c(tθ1)–c(tθ3).
- $A^{3\text{–}4}$ and $B^{2\text{–}3}$ are inherited from A^2, c(tθ13)–c(tθ15).
- A^4 and $B^{2\text{–}3}$ are inherited from A^3, c(tθ16)–c(tθ18).
- B^1 are inherited from B, c(tθ7)–c(tθ9).

(3) Functional reconstruction of cover media (RQ 3)

Section 4 proposes some timestamp rules of ADS files for the NTFS file system with Windows operating systems. Tracing the contact artifacts of cover media can provide useful information in a digital forensic investigation. Knowing timestamps might help decide on the follow-up investigation, produce actionable intelligence, and reserve in-depth forensic analysis for particular situations. For example, Rule 3 (original media) exhibits that practitioners can identify the AC-time of original media in Stage 2(b) or 3(b) and search for same/similar files with the same temporal values in other locations. Rule 7 (marked media) exhibits that there may be ADS operations or data hiding if the $SI.M-time of marked media is updated.



(**a**) Original

(**b**) Simplified

Figure 5. Relational reconstruction from temporal values and varieties (experiment).

5. Discussions and Analyses on Case Examples

In different stages, the inherited variety of cover media is observed to uncover hidden relations in this experiment. The analysis results of another file set in Section 5.2 (Case 2) is further examined to assess what changes, modifications, or operations have occurred.

5.1. Case 1

There are significant piracy problems taking place on eBay, Amazon, and various Websites. Taiwan is not the only place to get pirated items. In March 2020, a joint investigation by MPA (American-based Motion Picture Association), ACE (Alliance for Creativity and Entertainment), several local TV networks, and CIB (Criminal Investigation Bureau) ended with the arrest of two alleged operators for providing pirated movies and TV programs online. That video streaming site called "8maple.ru" was set up in 2014. The piracy site allowed users to download free movies and TV shows all over the world. It has infringed on an estimated US$33.21 million worth of copyrighted material. The operators have made money from the website advertisements of US$66.66 thousand per month [38]. It takes significant resources for the practitioner to track and fight piracy. The two criminals were arrested in Taoyuan, Taiwan, after 6-month surveillance and collection of evidence. The police identified 25 cloud servers, which were located in the United States, Canada, France, Ukraine, and Romania. The related 20 websites are also involved and blocked in this copyright infringement. Both files on clients and servers are guilty of content. Cellphones, computers, and Internet servers at the crime scene were seized during the arrest.

Case 1 was selected to illustrate the importance of contact artifacts, which can be applied to other cases. That case highlights the possibility of using contact artifacts for crime scene reconstruction. It allows the breakdown of the case into a set of claims and helps diverse evidence of different types that can be acquired at various sources in time [13]. The more sufficient contact artifacts can be found, the better relevant activities can be supported or refuted. The timestamp transfer of trace evidence is through the exchange contact of file operations [5]. The crackdown successfully probed the digital video content of illegal uploads and downloads. Practitioners discover the timestamp transfer of the event on the system. By examining the metadata of the first and last files on some specific dates, the entire period of the word-processing session could illustrate their guilty. It was revealed that their files were modified, accessed, or created during that period. This information was critical in refuting the innocence, as the metadata is consistent with their behaviors.

Moreover, the contact artifacts of file/Internet metadata can be found and used as temporal trace evidence in that cybercrime investigation [19]. File metadata is essential to carry significant value in cybercrime investigations but can be quite complex in structures, formats, and information [39]. That trace evidence can be valuable in court because it records essential activities on the file system. It also provides information about the authorship, editing time, or timestamps for accounting purposes. Timestamps might provide some clues to the investigative community at large. It could be adopted as an essential source to identify suspicious behaviors or establish an event timeline [12]. The file without the metadata may lose useful information when it is found [37]. Internet metadata includes Webpage and Browser metadata [36]. Webpage metadata for cloud services is in the form of meta tags, page titles, page headers, and meta descriptions. Valuable trace evidence about an email account or IP address may be included in some cases. Browser metadata shows the visited result of an Internet history page from a computer hard drive and is used extensively as forensic evidence.

5.2. Case 2

Criminals often handle data through various operations or techniques, which are difficult to predict. Case 2 looks for ways that data may be normally inaccessible or hidden either within the Word or text file for comparison. Timestamps are recorded on 11 September 2017. The researcher tries to assess what changes, modifications, or operations have occurred. In Tables 12 and 13, the inherited variety of cover media is illustrated as $\boldsymbol{W}$–$\boldsymbol{W}^7$ (Word file) and $\boldsymbol{T}$–$\boldsymbol{T}^7$ (text file). The criminal takes some of the following operations in this case [11].

Table 12. Timestamp observation on Word ADS operations.

Timestamp Rule	ADS Operation Steps	Original Media Time tθn	Inherited Variety	Temporal Value c(tθn)							
				\$SI				\$FN			
				E	M	A	C	E	M	A	C
1	C1.1:Word file creation	05:03:09(1)/ 05:03:10(1′)	$\boldsymbol{W}$	$\underline{1'}$	$\underline{1'}$	$\underline{1'}$	$\underline{1}$	$\underline{1'}$	$\underline{1'}$	$\underline{1'}$	$\underline{1}$
3	C2.1: Create data (text file) into the ADS of Word file	05:10:46(3)	$\boldsymbol{W^1}$	$\underline{3}$	$\underline{3}$	1′	1	1′	1′	1′	1
N/A	C3.1: Decompress Word file	09:44:27(5)	$\boldsymbol{W^2}$	$\underline{5}$	1′	$\underline{5}$	$\underline{5}$	$\underline{5}$	$\underline{5}$	$\underline{5}$	$\underline{5}$
3	C4.1: Create data (text file) into the ADS of Word file	09:50:26(7)	$\boldsymbol{W^3}$	$\underline{7}$	$\underline{7}$	5	5	5	5	5	5
3	C4.3: Create data (Word file) into the ADS of Word file	09:52:23(9)	$\boldsymbol{W^4}$	$\underline{9}$	$\underline{9}$	5	5	5	5	5	5
3	C4.5: Create data (PE file) into the ADS of Word file	09:54:36(11)	$\boldsymbol{W^5}$	$\underline{11}$	$\underline{11}$	5	5	5	5	5	5
3	C4.7: Create data (jpg file) into the ADS of Word file	09:56:28(13)	$\boldsymbol{W^6}$	$\underline{13}$	$\underline{13}$	5	5	5	5	5	5
6	C5.1: Extract the ADS from Word file	10:07:42(15)	$\boldsymbol{W^7}$	$\underline{13}$	$\underline{13}$	5	5	5	5	5	5
2/6	C6.1: Delete the ADS from Word file	10:09:00(17)	$\boldsymbol{W^8}$	$\underline{17}$	9	5	5	5	5	5	5

Note: N/A: no information.

Table 13. Timestamp observation on text ADS operations.

Timestamp Rule	ADS Operation Steps	Original Media Time tθn		Inherited Variety	Temporal Value c(tθn)							
					$SI				$FN			
					E	M	A	C	E	M	A	C
1	C1.2: Text file creation	05:03:20 (2)		$\boldsymbol{T}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$
3	C2.2: Create data (text file) into the ADS of text file	05:11:41(4)		$\boldsymbol{T^1}$	$\underline{4}$	$\underline{4}$	2	2	2	2	2	2
N/A	C3.2: Decompress text file	Typo [11]	05:03:20 (2)	$\boldsymbol{T^2}$	2	1′	2	2	2	2	2	2
		Correct	09:44:27 (5) = (6)		5	2	5	5	5	5	5	5
3	C4.2: Create data (text file) into the ADS of text file	09:50:58(8)		$\boldsymbol{T^3}$	$\underline{8}$	$\underline{8}$	5	5	5	5	5	5
3	C4.4: Create data (Word file) into the ADS of text file	09:52:57(10)		$\boldsymbol{T^4}$	$\underline{10}$	$\underline{10}$	5	5	5	5	5	5
3	C4.6: Create data (PE file) into the ADS of text file	09:55:10(12)		$\boldsymbol{T^5}$	$\underline{12}$	$\underline{12}$	5	5	5	5	5	5
3	C4.8: Create data (jpg file) into the ADS of text file	09:56:59(14)		$\boldsymbol{T^6}$	$\underline{14}$	$\underline{14}$	5	5	5	5	5	5
6	C5.2: Extract the ADS from text file	10:08:01(16)		$\boldsymbol{T^7}$	14	14	5	5	5	5	5	5
2/6	C6.2: Delete the ADS from text file	10:09:07(18)		$\boldsymbol{T^8}$	$\underline{18}$	14	5	5	5	5	5	5

Note: N/A: no information.

- Step C1. Word/txt file creation
- Step C2. Create data (text file) into the ADS of Word/text file
- Step C3. Decompress Word/text file
- Step C4. Create data (text, Word, PE, and jpg file) into the ADS of Word/text file
- Step C5. Extract the ADS from Word/text file
- Step C6. Delete the ADS from Word/text file

Criminals may randomly use various additional operations to hide their secret information. They may show the most diverse range of behaviors that make the cybercrime investigation task much challenging to utilize proper analysis tools or experiments to explore the fact. To gain meaningful results, this simplified Case 2 is designed and constructed to analyze the effects of timestamp rules. It requires much effort, patience, and time to experiment with possible operations on various systems and scenarios. There were not enough findings to assess or predict what kind of operations have occurred from the timestamp rules of cover media in Case 2. However, the researcher tries to evaluate this case from the following RQs.

(1) Finding timestamp rules from temporal values (RQ 1)

Finding timestamp rules from temporal values in ADS operations can still examine what file activities occurred on the computer during a particular time and analyze various auditing log files to correlate file operations with relevant events. The brief results of FTK analysis on ADS operations are illustrated in Tables 12 and 13, which meet the above-proposed rules (Rule 1, 2, 3, and 6) and represent the fundamental facts of the case.

- Rule 1. When original media are created, all timestamps are technically equaled in Step C1. A time delay also happens during the process.
- Rule 2. When users delete the ADS from Word/text files, the $SI.E-time is updated in Step C6. Even though the user has different operations, their timestamp rules are the same situations with Rule 2 (modification or overwriting).
- Rule 3. Creating data (text, Word, PE, and jpg file) into the ADS of Word/text file will update the $SI.EM-time of original media in Step C2 and C4. Showing the actual file content becomes essential to identify their former ADS operations (creation, modification, or overwriting).
- Rule 6. Extracting the ADS from Word/text file will keep any timestamps unchanged in Step C5 and C6. The $SI timestamp order on original media (Rule 6) still holds.

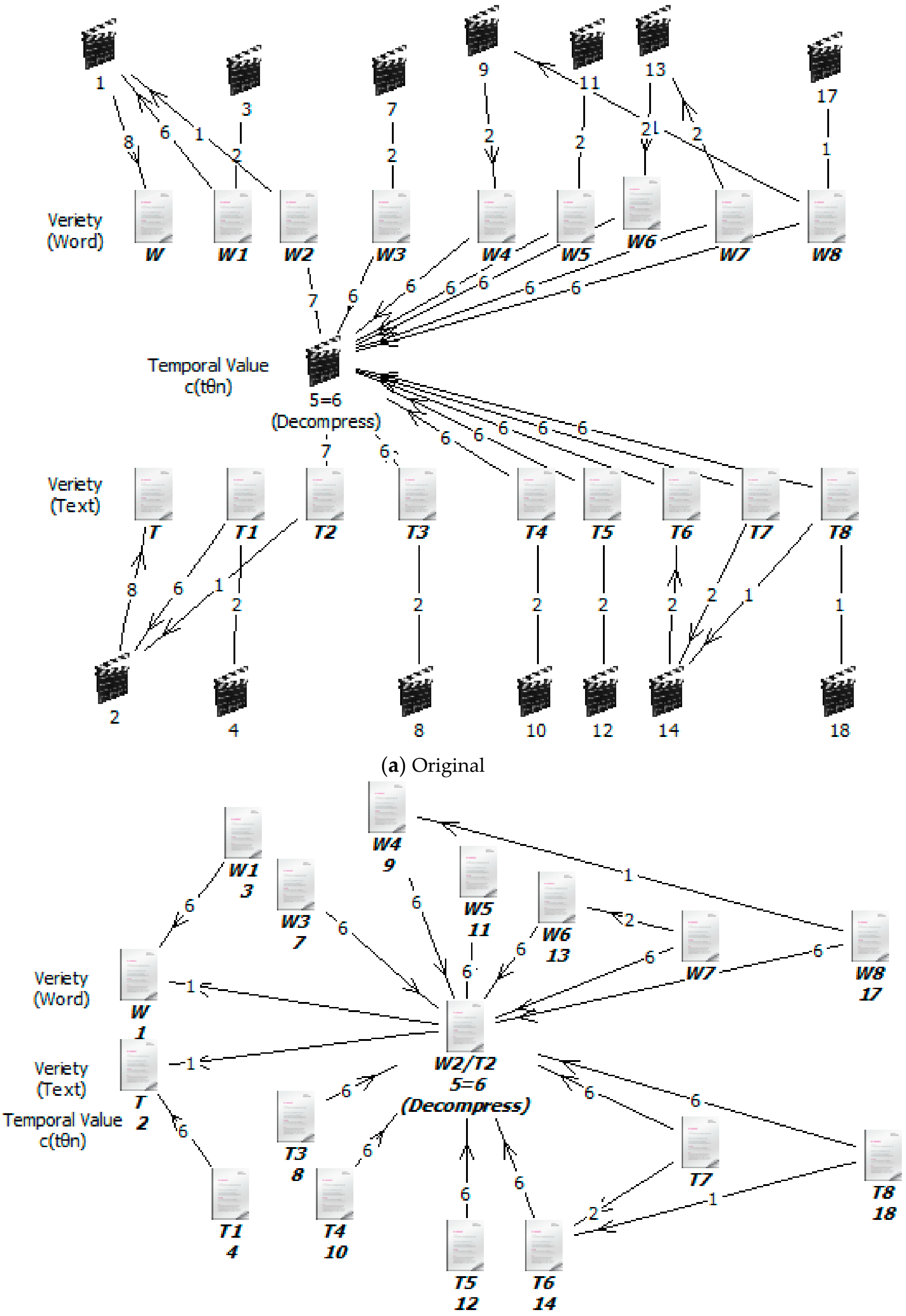
(2) Uncovering hidden relations in an inherited variety (RQ 2)

There are various ways a criminal can commit his crime or conceal his data. The researcher can still uncover hidden relations and predict where the contact artifacts of inherited variety will be located. The inherited variety can be the evidence dynamics of contact artifacts. Criminals are exploiting the convenience and anonymity of modern technologies to commit a diverse range of criminal activities. The researcher also analyzes the available evidence to looks for the presence of the predicted artifacts. However, some of the criminal operations are out of the scope of this paper. For example, Tables 12 and 13 illustrates the temporal values of $SI.AC-time and $FN.time in Step C4–C6 ($\boldsymbol{W^2}$–$\boldsymbol{W^8}$ and $\boldsymbol{T^2}$–$\boldsymbol{T^8}$) are inherited from Step C3 ($\boldsymbol{W^2}$ and $\boldsymbol{T^2}$).

Moreover, the researcher also uses IBM i2 Analyst's Notebook to analyze Tables 12 and 13 and discovers the visual contacts in Figure 6, which facilitate the relational reconstruction from the contact artifacts of temporal values. Figure 6a illustrates its original status. Figure 6b further removes the centralized W^2 to reduce the noise data and merges the related entities to provide a reduced view of information. Some divisible temporal attributes of contact artifacts happen below:

- W^1 is inherited from W.

- W^7 is inherited from W^6.
- W^8 is inherited from W^4.
- T^2 and T^1 are inherited from T.
- T^7 and T^8 are inherited from $T^{6.}$



(**a**) Original

(**b**) Simplified

Figure 6. Relational reconstruction from the contact artifacts of temporal values (Case 2).

(3) Tracing the contact artifacts of cover media (RQ 3)

The temporal attributes of digital files can exactly verify whether or not crimes are related to suspects and victims [37]. Practitioners can trace the contact artifacts of cover media. Practitioners can explore timestamp rules using case examples, which allow practical applications of crime scene reconstruction to real-world contexts [13]. After repeating these similar experiments, the researcher finds that: There is a c(tθ6) typo [11] in Step C3.2 since the researcher cannot find any former relation in Step C1.1 ($SI.M-time ≠ 1′). Moreover, Kao and Chan also have expressed that file decompression is similar to file creation, and $SI.M-time remains unchanged in Step C3 [11]. Then, the researcher can know that the temporal value c(tθ6) is equal to c(tθ5). It means that the user decompresses the Word/text file at the same time c(tθ5) in Step C3. The correct temporal value in Step C3.2 is illustrated in Table 13. This kind of evidence can be handled through file metadata or other sources to recreate events. For example, the value of $SI.M-time in Step C6.1, c(tθ9), shows that its source file is created from Step C4.3 (Table 12). Moreover, different file types or operations have their unique update timestamp patterns in Step C3. For instance, decompressing Word files will update their $SI.EAC-time and $FN-time. However, all timestamps of original media keep unchanged in decompressing .txt files.

5.3. Limitations

Every computer system action, including creating, modifying, or overwriting, will leave traces. Tracing the source items from the timestamps is possible. File content and its metadata are of equal interest to a practitioner, and the information in the metadata is highly dependent on their operations. The contact artifacts of inherited variety help practitioners trace the source items. Practitioners need a guide to understanding where and how they can discover concealed data quickly and retrieve it forensically. Then, a forensic investigation can put an equal amount of timestamp transfer to uncover hidden relations. Reversing some operations is possible from timestamp rules. There is always an ongoing investigative effort to extract the most useful digital evidence as efficiently as possible. This paper performs ADS operations, tests temporal attributes, and interprets timestamp rules. Practitioners still need to overcome many technical challenges, support the forensic data acquisition, and have greater access to digital evidence.

(1) The researcher cannot guarantee whether the timestamps have tampered.

Some forgeries may jeopardize the analysts and tampered digital evidence may fool its correct interpretation in a court of law [10]. Contact artifacts can provide a detailed description of the truth from other relevant sources [36]. Analyzing file metadata can explore an event to find something suspicious or abnormal. If these timestamps are overlooked, an incorrect conclusion or dire consequences could potentially be reached for the accused [3]. This paper did not take into account the applications that may manipulate timestamps to render the proposed rules invalid.

(2) Timestamp rules may change in different environments.

Temporal attributes have a high value in cybercrime investigations, especially when it comes to data hiding [27]. Various time changes may be represented differently across multiple user behaviors [3]. Every version of digital objects may have its unique timestamp rules. These proposed rules may change in different environments of digital objects. Practitioners should always test user behavior in suitable scenarios and analyze their difference so that they can avoid making mistakes in reconstructing crime scenes.

(3) Every cybercrime case is unique.

There is also no magic timestamp rules or strategies to assess what kinds of modifications or operations have occurred in a case. Various methods of handling files make it difficult for practitioners to examine digital evidence efficiently or effectively. It needs lots of knowledge, skills, abilities, hard work, and tough choices. The experimental contributions of this paper analyze temporal attributes in ADS operations, propose some timestamp rules in ADS operations, analyze their relationships on cover media, and collect digital trace evidence from crime scenes. It is possible to reverse some of their former operations from the temporal attributes of file metadata. However, it is impractical to assess every possible operation from some limited timestamp rules. Every cybercrime case is unique and somewhat different from each other. More experiments are necessary to extend more timestamp rules or meet the requirements of each case.

6. Conclusions

Data hiding prevents unauthorized access when computers have stored information. Various devices have all been used as digital assistance or concealment for communicating with others. ADS has posed significant challenges for practitioners to be executed without affecting their functionality, size, or display. The storage and handling of ADS will update some temporal attributes, which leave a trace for further investigation. The identical piece is also given in the temporal value c(tθn) as it can alert the practitioner of the ADS presence. This paper introduces a set of techniques for evaluating the performance in ADS operations, develops an experimental procedure for detecting them, and thus, plays a role in crime reconstruction. The forensic process plan effectively discovers the timestamp transfer of temporal attributes in a digital environment that can assist in detecting digital artifacts and exploring human behaviors from extracting temporal values to connected files or devices. Based on a sequence of controlled experiments, this paper observes the temporal attributes in ADS operations and performs a convincing forensic exchange analysis of digital evidence during a digital investigation. These experimental results can be further used to identify user behaviors and their sequential processes, where a sequence of events is involved. The empirical results of different scenarios in Section 5 suggest that the finding is useful in reconstructing events. The researcher performs a sequence of experiments to understand the contact artifacts of timestamp transfer. Overall, the results confirmed the findings on the existence of timestamp transfer. Namely, a practitioner can uncover hidden relations using timestamp rules from contact artifacts.

Researchers and practitioners need to identify temporal attributes, collect numerous contact artifacts, and collect relevant sources from a diversity of seized devices. Putting relevant data altogether and tracing the timestamp transfer will become a necessity during a cybercrime investigation. The more times an experiment is repeatedly evaluated with the same results, the more likely it is that the result is real. An independent practitioner should be able to examine those operations and achieve the same result repetitively. It eliminates conclusions that are based on what could be flukes. Although this paper is an initial beginning of the forensic exchange analysis of timestamp transfer, this domain needs more researches. More experiments on timestamps are needed to get a clear picture of forensic significance at hand. Future researches are going to be connected to test new case studies and reconstruct them from timestamp transfer viewpoints.

Funding: This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

Acknowledgments: Thanks are given to Yuan-Pei Chen (Chan) for assistance with the laboratory work and to anonymous reviewers for their constructive criticisms, which provided essential help in improving this paper.

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A. Experimental Steps in Stage 1 (Creation)

Stage 1(a). F Drive 1st Creation on Original Media

Step 1. F:\F1 Creation: (1) move to F drive, (2) press the rightmost button on a computer mouse, (3) add a new folder, and (4) rename the folder name as F1.

Step 2. F:\F1\T1.txt Creation: (1) open Notepad and create a new text document, (2) input some data, and (3) save the text file name as T1.

Step 3. F:\F1\W1.docx Creation: (1) open Microsoft Word and create a new text document, (2) input some data, and (3) save the Word file name as W1.

Stage 1(b). F Drive 1st ADS Creation on Marked Media

Step 4. F:\F1:EF-1.txt Creation: F:\> echo "EF-1.txt" > F1:EF-1.txt
Step 5. F:\F1\T1.txt:ET-1.txt Creation: F:\F1\> echo "ET-1.txt" > T1.txt:ET-1.txt
Step 6. F:\F1\W1.docx:EW-1.txt Creation: F:\F1\> echo "EW-1.txt" > W1.docx:EW-1.txt

Stage 1(c). G Drive 1st Creation on Original Media

Step 7. G:\F3 Creation: (1) move to G drive, (2) press the rightmost button on a computer mouse, (3) add a new folder, and (4) rename the folder name as F3.
Step 8. G:\F3\T3.txt Creation: (1) open Notepad and create a new text document, (2) input some data, and (3) save the text file name as T3.
Step 9. G:\F3\W3.docx Creation: (1) open Microsoft Word and create a new text document, (2) input some data, and (3) save the Word file name as W3.

Stage 1(d). G Drive 1st ADS Creation on Marked Media

Step 10. G:\F3:EF-1.txt Creation: G:\> echo "EF-1.txt" > F3:EF-1.txt
Step 11. G:\F3\T3.txt:ET-1.txt Creation: G:\F3\> echo "ET-1.txt" > T3.txt:ET-1.txt
Step 12. G:\F3\W3.docx:EW-1.txt Creation: G:\F3\> echo "EW-1.txt" > W3.docx:EW-1.txt

Stage 1(e). F Drive 2nd ADS Creation on Marked Media

Step 13. F:\F1:EF-2.txt Creation: F:\> echo "EF-2.txt" > F1:EF-2.txt
Step 14. F:\F1\T1.txt:ET-2.txt Creation: F:\F1\> echo "ET-2.txt" > T1.txt:ET-2.txt
Step 15. F:\F1\W1.docx:EW-2.txt Creation: F:\F1\> echo "EW-2.txt" > W1.docx:EW-2.txt

Appendix B. Experimental Steps in Stage 2 (Modification)

Stage 2(a). F Drive Modification on Original Media

Step 16. Rename F:\F1 as F:\F3 (F:\> rename F:\F1 F:\F3)
Step 17. Rename F:\F3\T1.txt as F:\F3\T3.txt (F:\> rename F:\F3\T1.txt F:\F3\T3.txt)
Step 18. Rename F:\F3\W1.docx as F:\F3\W2.docx (F:\> rename F:\F3\W1.docx F:\F3\W2.docx)

Stage 2(b). F Drive 1st ADS Modification on Marked Media

Step 19. F:\F3:EF-1.txt Modification: (1) F:\> notepad "F3:EF-1.txt," (2) modify data, and (3) save it.
Step 20. F:\F3\T3.txt:ET-1.txt Modification: (1) F:\F3\> notepad "T3.txt:ET-1.txt," (2) modify data, and (3) save it.
Step 21. F:\F3\W3.docx:EW-1.txt Modification: (1) F:\F3\> notepad "W3.docx:EW-1.txt," (2) modify data, and (3) save it.

Appendix C. Experimental Steps in Stage 3 (Overwriting)

Stage 3(a). F Drive Overwriting on Original Media

Step 22. G:\F3 Overwrite F:\F3 (copy and replace)
Step 23. G:\F3\T3.txt Overwrite F:\F3\T3.txt (copy and replace)
Step 24. G:\F3\W3.docx Overwrite F:\F3\W3.docx (copy and replace)

Stage 3(b). F Drive 1st ADS Overwriting on Marked Media

Step 25. F:\> type G:\F3:EF-1.txt > F3:EF-1.txt
Step 26. F:\F3\> type G:\F3\T3.txt:ET-1.txt > T3.txt:ET-1.txt
Step 27. F:\F3\> type G:\F3\W3.docx:EW-1.txt > W3.docx:EW-1.txt

References

1. Palmbach, D.; Breitinger, F. Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. *Forensic Sci. Int. Digit. Investig.* **2020**, *32S*, 300920. [CrossRef]
2. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G.; Benedetto, L. A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 277–305. [CrossRef]
3. Bang, J.; Yoo, B.; Lee, S. Analysis of Changes in File Time Attributes With File Manipulation. *Digit. Investig.* **2011**, *7*, 135–144. [CrossRef]
4. Willassen, S.Y. Methods for Enhancement of Timestamp Evidence in Digital Investigations. Ph.D. Thesis, Norwegian University of Science and Technology, Trondheim, Norway, January 2008; pp. 106–124.
5. Willassen, S.Y. Timestamp Evidence Correlation by Model Based Clock Hypothesis Testing. In Proceedings of the 1st International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide, Australia, 21–23 January 2008.
6. Šustr, J. Malware and the Possibilities of Its Evolution. Master's Thesis, VŠB—Technical University of Ostrava, Ostrava, Czech, 2019; pp. 17–22.
7. Krahl, K.M. Using Microsoft Word to Hide Data. Master's Thesis, Utica College, Utica, NY, USA, 2017; pp. 1–13.
8. Anson, S. *Applied Incident Response*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2020; pp. 311–318.
9. Mahajan, R. Stealth ADS: Enhanced Framework for Alternate Data Streams. In Proceedings of the 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 23–25 December 2016; pp. 1–5.
10. Schneider, J.; Wolf, J.; Freiling, F. Tampering with Digital Evidence is Hard: The Case of Main Memory Images. *Forensic Sci. Int. Digit. Investig.* **2020**, *32S*, 300924. [CrossRef]
11. Kao, D.Y.; Chan, Y.P. Identifying Temporal Patterns Using ADS in NTFS for Digital Forensics. *Adv. Intell. Syst. Comput.* **2018**, *733*, 273–285.
12. Stephenson, P. *Official (ISC)2®Guide to the Certified Cyber Forensics Professional (CCFP) Common Body of Knowledge (CBK)*; CRC Press: Boca Raton, FL, USA, 2014; pp. 293–404.
13. Franqueira, V.N.L.; Horsman, G. Towards Sound Forensic Arguments: Structured Argumentation Applied to Digital Forensics Practice. *Forensic Sci. Int. Digit. Investig.* **2020**, *32S*, 300923. [CrossRef]
14. Zola, F.; Bruse, J.L.; Eguimendia, M.; Galar, M.; Urrutia, R.O. Bitcoin and Cybersecurity: Temporal Dissection of Blockchain Data to Unveil Changes in Entity Behavioral Patterns. *Appl. Sci.* **2019**, *9*, 5003. [CrossRef]
15. Shavers, B. *Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*; Syngress Publishing: Waltham, MA, USA, 2013; pp. 85–122.
16. Inman, K.; Rudin, N. *Principles and Practice of Criminalistics: The Profession of Forensic Science*; CRC Press: Boca Raton, FL, USA, 2000; pp. 113–192.
17. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed.; Elsevier Inc.: Amsterdam, The Netherlands, 2011; pp. 187–464.
18. Casey, E. *Handbook of Digital Forensics and Investigation*; Elsevier Inc.: Amsterdam, The Netherlands, 2010; pp. 209–300.
19. Carrier, B. *File System Forensic Analysis*; Pearson Education: London, UK, 2005; pp. 173–396.
20. Kao, D.Y.; Lin, H.C. Dissecting Alternate Data Streams in Anti-Digital Forensics. *Law Enforc. Rev.* **2017**, *13*, 39–68.
21. Raggo, M.; Hosmer, C. *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices, and Network Protocols*; Syngress Publisher: Waltham, MA, USA, 2012; pp. 133–166.
22. Mahant, S.H.; Meshram, B.B. ADS Examiner: Tool for NTFS Alternate Data Streams Forensics Analysis. *Int. J. Eng. Res. Technol. IJERT* **2012**, *1*, 1–10.
23. Microsoft Corporation. API Index for Desktop Windows Applications. Available online: https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list (accessed on 30 April 2020).
24. Microsoft Corporation. File Times. Available online: https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times (accessed on 30 April 2020).
25. Microsoft Corporation. [SMS-FSA]: File System Algorithms. Available online: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fsa/860b1516-c452-47b4-bdbc-625d344e2041 (accessed on 30 April 2020).

26. Shook, S. *Cybercrime Investigation Body of Knowledge*; CIBOK Editor Committee: Tokyo, Japan, 2017; pp. 155–200.
27. Đuranec, A.; Topolčić, D.; Hausknecht, K.; Delija, D. Investigating File Use and Knowledge with Windows 10 Artifacts. In Proceedings of the 2019 42nd IEEE International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019.
28. Moreno, J.; Serrano, M.A.; Fernandez, E.B.; Fernández-Medina, E. Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies. *Appl. Sci.* **2020**, *10*, 724. [CrossRef]
29. Nowostawski, M.; Tøn, J. Evaluating Methods for the Identification of Off-Chain Transactions in the Lightning Network. *Appl. Sci.* **2019**, *9*, 2519. [CrossRef]
30. Din, R.; Mahmuddin, M.; Qasim, A.J. Review on Steganography Methods in Multi-Media Domain. *Int. J. Eng. Technol.* **2019**, *8*, 288–292.
31. Hassan, N.A.; Hijazi, R. *Data Hiding Techniques in Windows OS. A Practical Approach to Investigation and Defense*; Syngress Publisher: Cambridge, MA, USA, 2016; pp. 267–289.
32. Ho, S.M.; Kao, D.Y.; Wu, W.Y. Following the breadcrumbs: Timestamp pattern identification for cloud forensics. *Digit. Investig.* **2018**, *24*, 79–94. [CrossRef]
33. Kao, D.Y.; Chen, Y.P.; Shih, N.H. Reconstructing ADS Data Hiding in Windows NTFS: A Temporal Analysis. *Digit. Investig.* **2018**, *26*, S137. [CrossRef]
34. Akhgar, B.; Staniforth, A.; Bosco, F. *Cyber Crime and Cyber Terrorism Investigator's Handbook*; Elsevier Publishing: Amsterdam, The Netherlands, 2014; pp. 88–90.
35. Microsoft Corporation. File System Behavior in the Microsoft Windows Environment. Available online: http://download.microsoft.com/download/4/3/8/43889780-8d45-4b2e-9d3a-c696a890309f/filesystembehavioroverview.pdf (accessed on 30 April 2020).
36. Bunting, S. *EnCase Computer Forensics the Official EnCE Certified Examiner Study Guide*, 3rd ed.; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2012; pp. 33–88.
37. Lee, W.Y.; Kim, K.H.; Lee, H. Extraction of Creation-Time for Recovered Files on Windows FAT32 File System. *Appl. Sci.* **2019**, *9*, 5522. [CrossRef]
38. Criminal Investigation Bureau. News Releases. Available online: https://www.cib.gov.tw/News/Detail/42669 (accessed on 30 April 2020).
39. Kävrestad, J. *Guide to Digital Forensics—A Concise and Practical Introduction*; Springer International Publishing: Cham, Switzerland, 2017; pp. 3–8.