GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Windows Forensic Analysis (Forensics 500)"
at http://www.giac.org/registration/gcfe

Detection of Backdating the System Clock in Windows

GIAC GCFE Gold Certification

Author: Xiaoxi Fan, xfan@strozfriedberg.com
Advisor: Barbara L. Filkins
Accepted: March 12, 2017

March 12, 2017

Abstract

In the digital forensic industry, evidence concerning date and time is a fundamental part of many investigations. As one of the most commonly used anti-forensic approaches, system backdating has appeared in more and more investigations. Since the system clock can be set back manually, it is important for investigators to identify the reliability of date and time so as to make further decision. However, there is no simple way to tell whether the system clock has been backdated or tampered especially when it was subsequently reset to the correct time. There are a variety of artifacts to detect the behavior of backdating the system clock. If the investigator needs to prove the hypothesis that "the system clock has not been backdated," he or she must examine multiple artifacts for corroboration.

This paper presents three categories of related objects, showing how they work together in detecting system clock backdating: (1) system artifacts (e.g. Windows event log, $MFT, $Logfile, $UsnJrnl, Volume Shadow Copy, $STDINFO and $FILENAME timestamps, and Windows update logs); (2) application artifacts (e.g. antivirus update log and cloud storage sync log); and (3) Internet artifacts (e.g. Internet history and email). The paper intends to put together these artifacts and serve as a reference for investigators to detect system clock backdating.

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

1. Introduction

A timestamp is a recorded representation of a specific moment in time (Willassen, 2008), which is an important attribute to reflect certain changes to the file. The Windows operating system records the MAC timestamps of an individual file, an acronym that refers to the last modification time, access time, and creation time, respectively (Farmer, 2000). These timestamps can provide valuable information about what programs and files are used on Windows operating system. Timestamps are updated in accordance to the BIOS or operating system clock. They can provide a detailed sequence of the events that took place on the system and can help reconstruct the events to support the processes of computer forensics and incident response (Buchholz, Tjaden, 2007). In most investigations, we need to determine what happened to the system and when by looking into the timestamp attributes of the file. If the system clock is not accurate, it will affect the reliability of the timestamp attributes.

For example, we encountered a case that a former employee was suspected of stealing the intellectual property of the company. After this employee had known that his computer would be seized, he backdated the system clock to one-week prior, deleted a large number of files, and then copied and pasted some insignificant pictures multiple times to overwrite the deleted files. Since the system clock had been backdated, all records of the deletion and copy activities indicated the actions happened one week ago, intending to mislead the result of any investigation. Therefore, to obtain the reliable time information, an investigator must make sure the system clock is accurate and has never been backdated.

Previous researchers have focused on the timestamps in digital forensics. Willassen proposed a method to enhance the use of timestamps as evidence, by formulating hypotheses about clocks and testing them for consistency with observed timestamps (Willassen, 2008). Chow proposed a set of rules of timestamps to detect commonly used operations by end users, such as copy, delete, and download (Chow, 2007). Both these works focus on the use of timestamps in digital investigations, which require reliable time information. However, there is no systematic research about measuring the reliability of the timestamps, such as how to tell whether or not t

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

backdating or tampering with the system clock has occurred. This paper aims to analyze different kinds of artifacts to help investigators detect system clock backdating and tampering.

2. Methodology

A variety of sources provide timestamps: file system metadata, system logs, application data, and network data. By consolidating the experiences acquired from digital forensic investigations, some familiar artifacts on Windows operating system and NTFS file system were analyzed to find the indicators of system clock backdating and tampering, specifically Windows Event Log and $MFT.

We first created a test environment on a workstation, installing a set of commonly used applications to simulate a production environment. We then backdated the system clock and adjusted it back to the correct time for several times to leave a trace of evidence in various kinds of artifacts for analysis. The test image was searched to discover any logs which contain blocks of regularly recorded timestamps.

In normal operations, new timestamps are usually recorded be an increasing sequence. Any timestamp out of sequence possibly indicates the system has been backdated. This method is to search all the data on disk level to find potential indicators of system clock backdating and tampering.

3. Hypothetical Rules and Experiments

We observed and examined three categories of the objects: 1) system, 2) application and 3) Internet. We hypothesized a set of rules for each object that could be used to determine whether backdating and tampering with the system clock had occurred. By simulating different scenarios of system clock backdating and tampering, these experiments can help prove that the hypothetical rules work successfully to detect system clock backdating and tampering.

Xiaoxi Fan, xfan@strozfriedberg.com

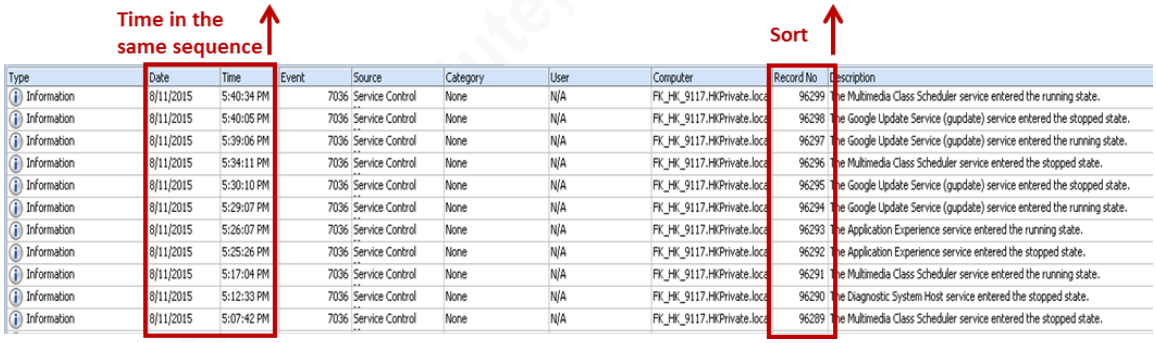
© 2017 The SANS Institute Author retains full rights.

3.1. System Artifacts

3.1.1. Windows Event Log – System Log

1. Record No & Date and Time

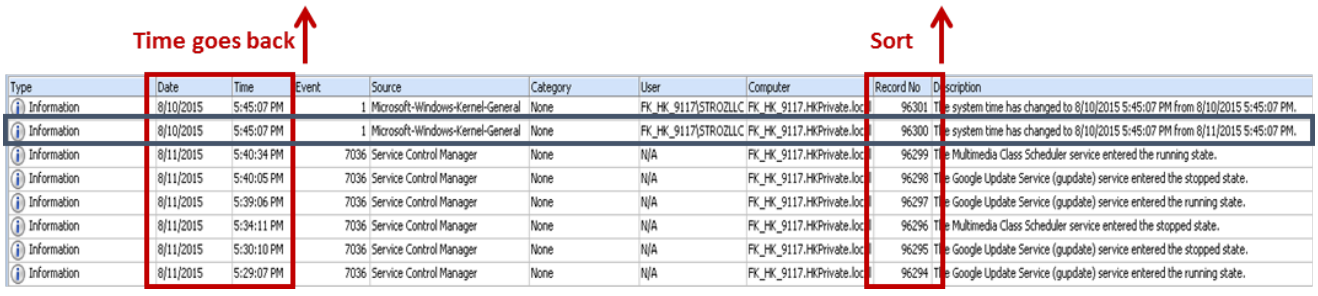
Each event log record has a Record No. Each Record No is sequential in increasing order according to time and can be distinguished from each other. The latest (i.e., most recent) event record is assigned the largest Record No. as shown in Figure 1. The record with the highest Record No has been produced after the record with the lowest Record No. As the Record No increases, the Date and Time column should increase as well.



Type	Date	Time	Event	Source	Category	User	Computer	Record No	Description
Information	8/11/2015	5:40:34 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96299	The Multimedia Class Scheduler service entered the running state.
Information	8/11/2015	5:40:05 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96298	The Google Update Service (gupdate) service entered the stopped state.
Information	8/11/2015	5:39:06 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96297	The Google Update Service (gupdate) service entered the running state.
Information	8/11/2015	5:34:11 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96296	The Multimedia Class Scheduler service entered the stopped state.
Information	8/11/2015	5:30:10 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96295	The Google Update Service (gupdate) service entered the stopped state.
Information	8/11/2015	5:29:07 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96294	The Google Update Service (gupdate) service entered the running state.
Information	8/11/2015	5:26:07 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96293	The Application Experience service entered the running state.
Information	8/11/2015	5:25:26 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96292	The Application Experience service entered the stopped state.
Information	8/11/2015	5:17:04 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96291	The Multimedia Class Scheduler service entered the running state.
Information	8/11/2015	5:12:33 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96290	The Diagnostic System Host service entered the stopped state.
Information	8/11/2015	5:07:42 PM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.loca	96289	The Multimedia Class Scheduler service entered the stopped state.

Figure 1: Standard System Event Log

When the Record No increases but the Date and Time is backdated, this is a sign that the system clock has been backdated (Figure 2).



Type	Date	Time	Event	Source	Category	User	Computer	Record No	Description
Information	8/10/2015	5:45:07 PM	1	Microsoft-Windows-Kernel-General	None	FK_HK_9117\STROZLLC	FK_HK_9117.HKPrivate.loca	96301	The system time has changed to 8/10/2015 5:45:07 PM from 8/10/2015 5:45:07 PM.
Information	8/10/2015	5:45:07 PM	1	Microsoft-Windows-Kernel-General	None	FK_HK_9117\STROZLLC	FK_HK_9117.HKPrivate.loca	96300	The system time has changed to 8/10/2015 5:45:07 PM from 8/11/2015 5:45:07 PM.
Information	8/11/2015	5:40:34 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96299	The Multimedia Class Scheduler service entered the running state.
Information	8/11/2015	5:40:05 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96298	The Google Update Service (gupdate) service entered the stopped state.
Information	8/11/2015	5:39:06 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96297	The Google Update Service (gupdate) service entered the running state.
Information	8/11/2015	5:34:11 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96296	The Multimedia Class Scheduler service entered the stopped state.
Information	8/11/2015	5:30:10 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96295	The Google Update Service (gupdate) service entered the stopped state.
Information	8/11/2015	5:29:07 PM	7036	Service Control Manager	None	N/A	FK_HK_9117.HKPrivate.loca	96294	The Google Update Service (gupdate) service entered the running state.

Figure 2: Standard System Event Log with Possible Backdating

2. Source & Event ID

Whenever a change to the system clock occurs, a corresponding record will be created in the system event log with Source as “Microsoft Windows Kernel General” and

© 2017 The SANS Institute Author retains full rights.

Event ID as 1. As shown in Figure 2, Record 96300 is a record of system clock change, providing the details as "The system time has changed to 8/10/2015 5:45:07 PM from 8/11/2015 5:45:07 PM" by user "STROZLLC." The change of time zone (without a change in date and time) is also recorded in the event log. After changing, all date and time in previous records are shown in current time zone (Figure 3).

Type	Date	Time	Event	Source	Category	User	Computer	Record No	Description
Information	8/10/2015	9:49:35 AM	1	Microsoft-Windows-K	None	FK_HK_9117\STROZLLC	FK_HK_9117.HKPrivate.local	96307	The system time has changed to 8/10/2015 9:49:35 AM from 8/10/2015 9:49:35 AM.
Information	8/10/2015	9:47:25 AM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.local	96306	The Multimedia Class Scheduler service entered the stopped state.
Information	8/10/2015	9:46:02 AM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.local	96305	The Virtual Disk service entered the stopped state.
Information	8/10/2015	9:46:02 AM	4	Virtual Disk Service	None	N/A	FK_HK_9117.HKPrivate.local	96304	Service stopped.
Information	8/10/2015	9:45:55 AM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.local	96303	The Virtual Disk service entered the running state.
Information	8/10/2015	9:45:55 AM	3	Virtual Disk Service	None	N/A	FK_HK_9117.HKPrivate.local	96302	Service started.
Information	8/10/2015	9:45:07 AM	1	Microsoft-Windows-K	None	FK_HK_9117\STROZLLC	FK_HK_9117.HKPrivate.local	96301	The system time has changed to 8/10/2015 9:45:07 AM from 8/10/2015 9:45:07 AM.
Information	8/10/2015	9:45:07 AM	1	Microsoft-Windows-K	None	FK_HK_9117\STROZLLC	FK_HK_9117.HKPrivate.local	96300	The system time has changed to 8/10/2015 9:45:07 AM from 8/11/2015 9:45:07 AM.
Information	8/11/2015	9:40:34 AM	7036	Service Control	None	N/A	FK_HK_9117.HKPrivate.local	96299	The Multimedia Class Scheduler service entered the running state.

Figure 3: System Event Log with Backdating

Event log has a default size of 512KB in Windows XP, while in both Windows Vista and Windows 7 the default size is 20MB (Lee, 2011). Once the log is full, it goes back to the beginning implementing a first-in-first-out overwriting process of old records.

The easiest way to tell whether or not the system clock has been changed is to examine the event logs. However, investigators need to pay attention that to the fact that Window may have overwritten old event records with newer ones as well as the possibility that an attacker or a user can delete the event logs. If there is no trace in event logs of the system clock having been changed, this may be due to the event log record has been overwritten or deleted. It is possible to find out the deleted event logs by recovering them from unallocated space. If there is no result from the recovery, the investigators may want to assess other artifacts introduced in the following sections, since different artifacts can maintain the data with different time periods.

3.1.2. Windows Event Log – Security Log

The security event log will contain the same information, if system auditing, normally off by default, is enabled for system events. Figure 4 shows an example of time change record in the security event log in Windows 7 system. The system records the previous and new times, where the Source is "Microsoft Windows Security Auditing," the Category is "Security State Change," and the Event ID is 4616. In

© 2017 The SANS Institute Author retains full rights.

Windows XP, the Event ID for system clock change is 520, which appears along with the Event ID 577 (privilege use logging) when manually changing the system time.

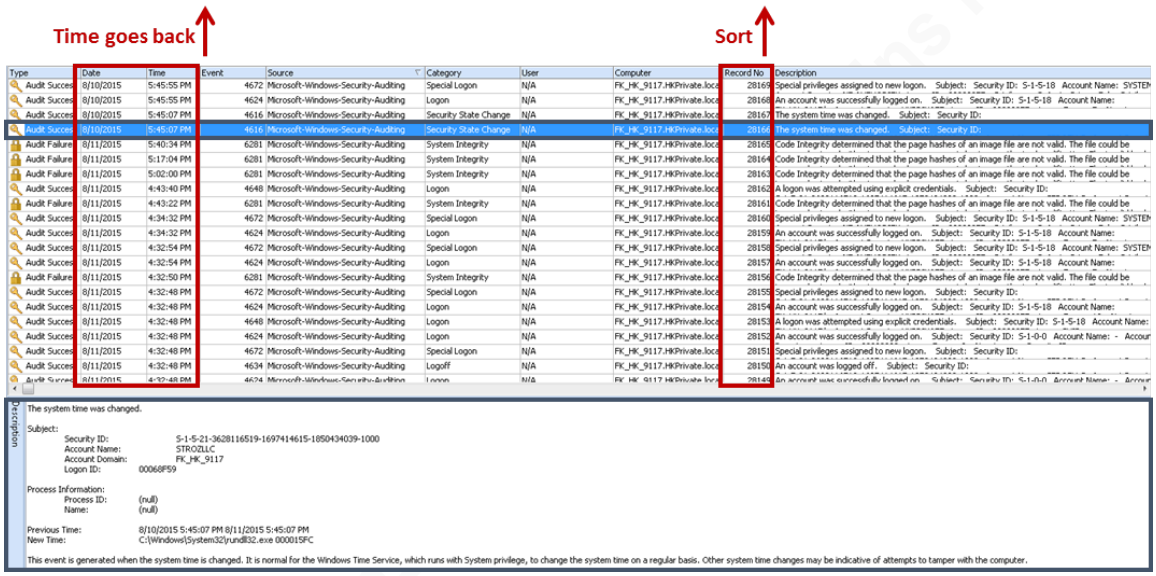


Figure 4: Time Change Record in the Security Log

If the auditing records are sorted by Record No, we see that the dates do not align. In this case, we can say that possible changes to the system clock have occurred.

3.1.3. NTFS $LogFile

In NTFS, journal file transactions are labeled with a number called Logical Sequence Number (LSN) that increases through the lifetime of the file system. The functioning of the journaling feature in NTFS depends on this number being strictly increasing. A higher LSN will be set for each new log record written. So the sequence of LSN indicates the actual time sequence of the actions.

After parsing the $LogFile using Triforce ANJP (Triforce, 2014), we do the following selection from the table logfile_event_ref. As shown in Figure 5, in normal situation, the MFT modified time (column ie_mft_m_dt) should increase as the LSN (column chg_lsn) becomes larger.

select loge_event_id, chg_name, chg_lsn, ie_c_dt, ie_m_dt, ie_mft_m_dt, ie_a_dt from logfile_event_ref where loge_event_id="Creations" order by chg_lsn;

In column loge_event_id, only the events “Creations” are considered, and others such as “Deletions” are filtered out. The reason is that for “Deletions,” the time attributes

© 2017 The SANS Institute Author retains full rights.

will not be updated to the current system clock. So if "Deletions" are included, the column ie_mft_m_dt may not be in increasing time sequence.

The file created time (column ie_c_dt) may not be in increasing time sequence. For example, when a file text.txt is open, and its corresponding LNK file already exists, the corresponding LNK file will be updated, and the modified time, accessed time, MFT modified time of the LNK file will be updated to the current system clock and the created time remains no change. We will compare MFT modified time to the LSN as the created time may not be in increasing time sequence as new actions are logged.

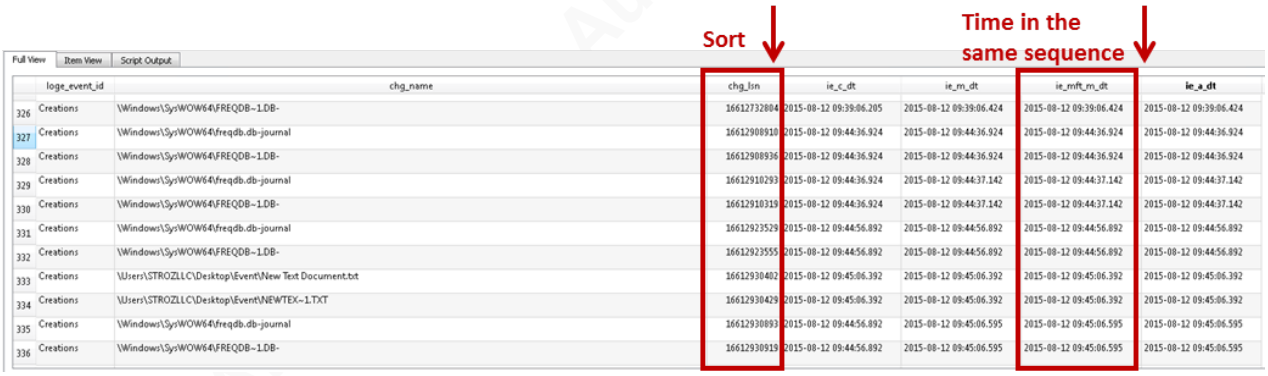


Figure 5: Normal Situation

As shown in Figure 6, the records are sorted according to LSN in ascending order. When backdating of the system clock occurs, we can identify it by recognizing the backdated MFT modified time (column ie_mft_m_dt).

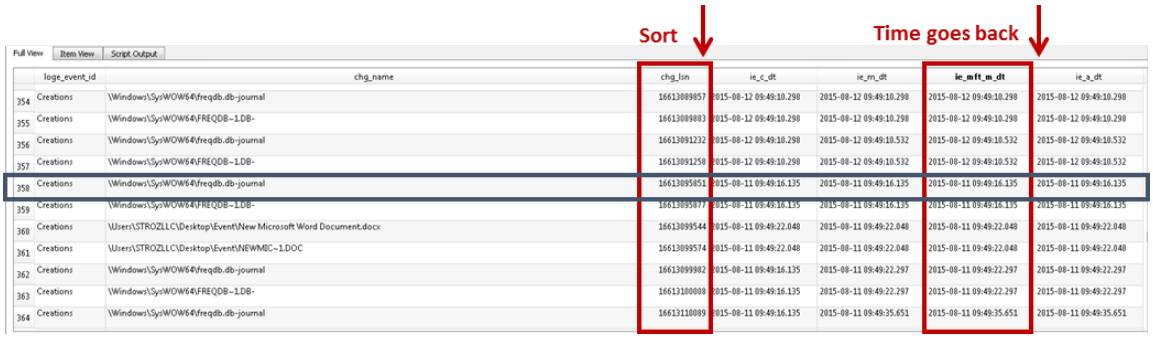


Figure 6: System Backdated

The major drawbacks to this method are that the journal file has a limited size and that logging works in a circular fashion. New records are added to the end of the file until the log reaches its full capacity. Then, the system frees up space for more recent

© 2017 The SANS Institute Author retains full rights.

records, deleting the old records. Compared to $LogFile, $UsnJrnl maintains more records. We will discuss this in the next. Our test machine was in active use for eight to nine hours per day, supporting actions like file open, creation, modification, copy, deletion and application running. It was in non-active use for the remaining time. We found that $UsnJrnl will keep records for 1 to 2 days while $LogFile 2.5 to 3 hours.

3.1.4. NTFS $UsnJrnl

NTFS $UsnJrnl sequentially stores records in the same manner as $LogFile. After parsing $UsnJrnal, in table usn_event_ref, column ur_usn is Update Sequence Number (USN). The USN information in each record determines its order. The latest record has the largest USN with the sequence of USN indicating the actual time sequence of the actions. Column ur_datetime is USN record date and time. Therefore, in a normal situation, as ur_usn increases, ur_datetime should be in increasing sequence (Figure 7).

Sort ↓ Time in the same sequence ↓

1	usne_event_id	ure_fullname	ur_usn	ur_record_offset	ur_transaction_count	ur_datetime
14011	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.Case	4357933552	4357933552	148781	08/24/2015 04:43
14012	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.cbak	4357933648	4357933648	148781	08/24/2015 04:43
14013	Renames_Moves	\Program Files\EnCase6\Backup\test2.1.cbak	4357933824	4357933824	148782	08/24/2015 04:43
14014	Renames_Moves	\Program Files\EnCase6\Backup\test2.x.cbak	4357933912	4357933912	148782	08/24/2015 04:43
14015	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.cbak	4357934088	4357934088	148783	08/24/2015 04:43
14016	Renames_Moves	\Program Files\EnCase6\Backup\test2.1.cbak	4357934176	4357934176	148783	08/24/2015 04:43
14017	Deletions	\Program Files\EnCase6\Backup\test2.x.cbak	4357934352	4357934352	148784	08/24/2015 04:43
14018	Creations	\Windows\SysWOW64\freqdb.db-journal	4357948112	4357948112	148849	08/24/2015 04:44
14019	Deletions	\Windows\SysWOW64\freqdb.db-journal	4357948576	4357948576	148850	08/24/2015 04:44
14020	Creations	\Program Files\EnCase6\Backup\test2.0.Case	4358006032	4358006032	149115	08/24/2015 04:48
14021	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.Case	4358006416	4358006416	149116	08/24/2015 04:48
14022	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.cbak	4358006512	4358006512	149116	08/24/2015 04:48
14023	Renames_Moves	\Program Files\EnCase6\Backup\test2.1.cbak	4358006688	4358006688	149117	08/24/2015 04:48
14024	Renames_Moves	\Program Files\EnCase6\Backup\test2.x.cbak	4358006776	4358006776	149117	08/24/2015 04:48
14025	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.cbak	4358006952	4358006952	149118	08/24/2015 04:48
14026	Renames_Moves	\Program Files\EnCase6\Backup\test2.1.cbak	4358007040	4358007040	149118	08/24/2015 04:48
14027	Deletions	\Program Files\EnCase6\Backup\test2.x.cbak	4358007216	4358007216	149119	08/24/2015 04:48
14028	Creations	\Program Files\EnCase6\Backup\test2.0.Case	4358077824	4358077824	149446	08/24/2015 04:53
14029	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.Case	4358078208	4358078208	149447	08/24/2015 04:53

Figure 7: $USN.Jml Normal Situation

When the sequence of ur_datetime is not consistent with ur_usn, it indicates the system clock has been backdated (Figure 8). Here, the system clock has been backdated seven days on 8/17/2015 06:57.

© 2017 The SANS Institute Author retains full rights.

Sort ↓ Time goes back ↓

1	usne_event_id	ure_fullname	ur_usn	ur_record_offset	ur_transaction_count	ur_datetime
15064	Renames_Moves	\Program Files\EnCase6\Backup\test2.x.cba	4359968328	4359968328	158336	08/24/2015 06:55
15065	Renames_Moves	\Program Files\EnCase6\Backup\test2.0.cba	4359968504	4359968504	158337	08/24/2015 06:55
15066	Renames_Moves	\Program Files\EnCase6\Backup\test2.1.cba	4359968592	4359968592	158337	08/24/2015 06:55
15067	Deletions	\Program Files\EnCase6\Backup\test2.x.cba	4359968768	4359968768	158338	08/24/2015 06:55
15068	Creations	\Windows\SysWOW64\freqdb.db-journal	4359992640	4359992640	158449	08/24/2015 06:57
15069	Deletions	\Windows\SysWOW64\freqdb.db-journal	4359993104	4359993104	158450	08/24/2015 06:57
15070	Creations	\Windows\SysWOW64\freqdb.db-journal	4359993280	4359993280	158452	08/24/2015 06:57
15071	Deletions	\Windows\SysWOW64\freqdb.db-journal	4359993744	4359993744	158453	08/24/2015 06:57
15072	Creations	\Windows\Prefetch\RUNDLL32.EXE-B811457	4359995216	4359995216	158461	08/17/2015 06:57
15073	Creations	\Windows\SysWOW64\freqdb.db-journal	4360013864	4360013864	158546	08/17/2015 06:58
15074	Deletions	\Windows\SysWOW64\freqdb.db-journal	4360014328	4360014328	158547	08/17/2015 06:58
15075	Creations	\Users\STROZLLC\Desktop\thumb\New Text	4360015152	4360015152	158552	08/17/2015 06:59
15076	Creations	\Windows\SysWOW64\freqdb.db-journal	4360015576	4360015576	158554	08/17/2015 06:59
15077	Deletions	\Windows\SysWOW64\freqdb.db-journal	4360016048	4360016048	158555	08/17/2015 06:59
15078	Creations	\Windows\SysWOW64\freqdb.db-journal	4360016224	4360016224	158557	08/17/2015 06:59

Figure 8: $USN.Jml System Backdated

In $UsnJrnl, there is no need to filter out events like “Deletions” or “Renames_Moves” since ur_datetime is the date and time when the event occurs. Column ur_record_offset is the offset of the record within the USN Journal (the same value as in ur_usn). Column ur_transaction_count is the transaction number (new transaction starts after a Close Reason) which is also in increasing sequence when adding a new record.

Unlike $LogFile, $UsnJrnl does not overwrite old records, but it uses the concept of the sparse file (Oh, 2013). New records are added at the end of $UsnJrnl. When the size of the data space is bigger than the defined maximum size in $UsnJrnl setting, old records will be paged out to unallocated space, and it is possible to recover these old records. According to previous research (Oh, 2013), it is possible to retrieve old records from several months or a year ago. These recovered USN records are a useful resource to detect system backdating happened a long time ago.

3.1.5. WindowsUpdate Log

The WindowsUpdate.log, kept by the Windows update process at C:\Windows\WindowsUpdate.log, can also be used to infer the system clock change. The latest record is written at the end of the log. In a typical situation, the timestamp of these entries increases when newer ones are created (Figure 9).

© 2017 The SANS Institute Author retains full rights.

Records are regularly written into the log according to the time provided by the system clock. Backdating of the system clock is indicated if the time sequence of these records goes backward in a given period. In Figure 10, since the time of the records is not in increasing order, we can tell the system clock has been backdated one day at 08/19/2015 12:23.

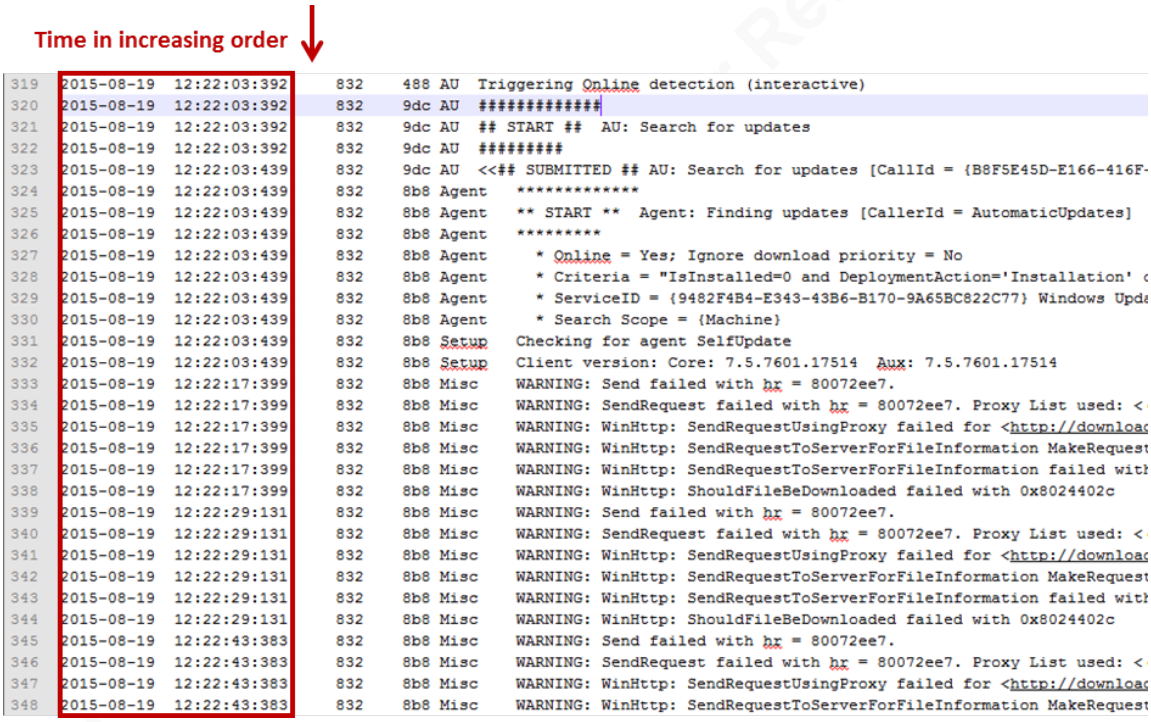


Figure 9: WindowsUpdate.log Normal Situation

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

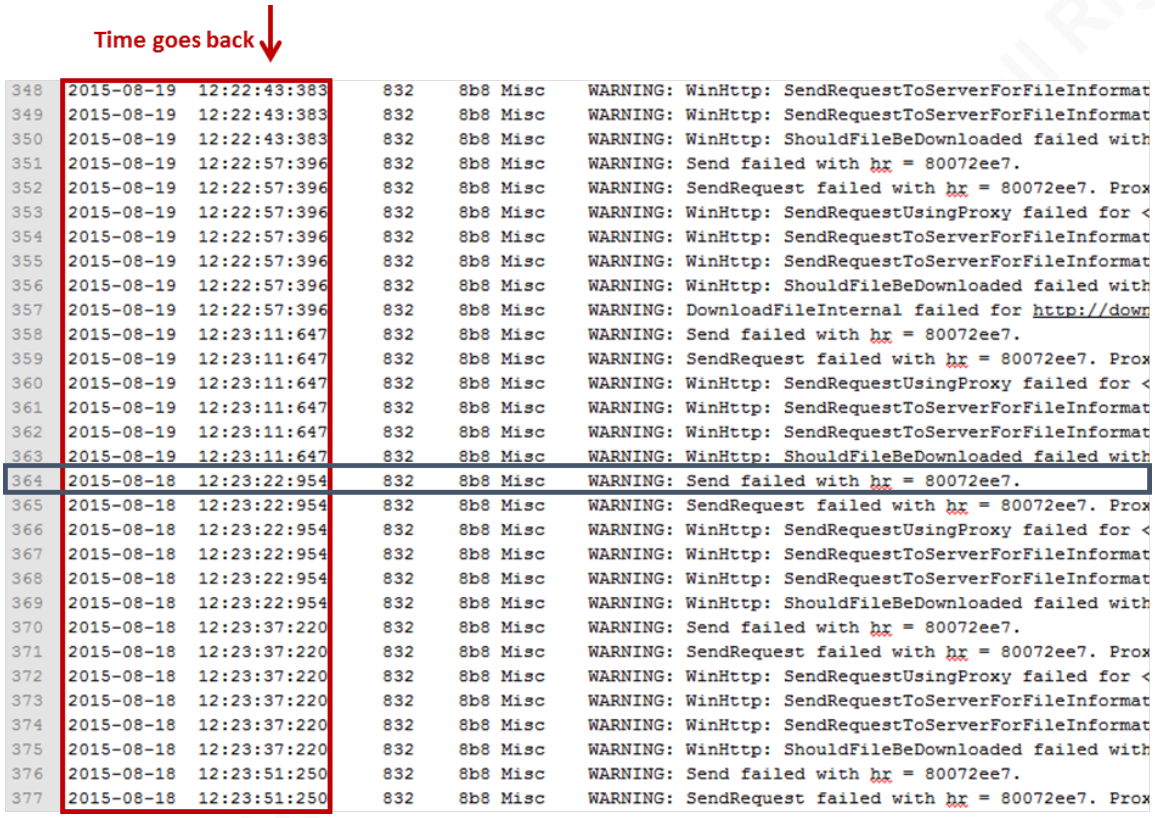


Figure 10: WindowsUpdate.log System Backdating

WindowsUpdate.log has a maximum physical size of 2MB, after which it automatically rolls over. The history contained in the file will be dependent upon how many entries have been generated in the 2MB. The Windows Update Agent, which supports automated patch delivery and installation, also writes to this log. Thus, the number of log entries depends on the configuration of Windows Update. With automatic updating is on, the log file may contain about one month of entries. With automatic updating turned off, the log file may contain several months of entries.

3.1.6. Volume Shadow Copy

Volume shadow copy is a process that backs up the system volume, which can be created by the operating system automatically or the end user manually. Windows Vista or Windows 7 keeps approximately 20 volume shadow copies under C:\System Volume Information. For a machine used daily on AC power without entering an idle state, we expect that a volume shadow copy is created every 1 to 2 days on Windows Vista and

© 2017 The SANS Institute Author retains full rights.

every 7 to 8 days on Windows 7. The actual frequency may be higher due to it can be created during software installation or by the end user manually (Szynalski, 2009).

In a typical situation, the names of volume shadow copy GUIDs are similar for a particular time. In Figure 11, the names of volume shadow copy GUIDs created in 2016 are similar to each other, while they are quite different from the one created in 2013.

Name	File Created	Last Accessed	Last Written	Entry Modified
MountPointManagerRemoteDatabase	27/02/13 04:47:02	27/02/13 04:47:02	27/02/13 04:47:02	27/02/13 04:47:02
SPP	26/02/13 20:56:14	15/06/16 11:16:23	15/06/16 11:16:23	15/06/16 11:16:23
Syscache.hve	27/02/13 04:47:58	15/06/16 11:19:07	15/06/16 11:19:07	15/06/16 11:19:02
Syscache.hve.LOG1	27/02/13 04:47:58	27/02/13 04:47:58	15/06/16 11:19:02	15/06/16 11:19:02
Syscache.hve.LOG2	27/02/13 04:47:58	27/02/13 04:47:58	27/02/13 04:47:58	27/02/13 04:47:58
tracking.log	27/02/13 04:47:55	27/02/13 04:47:55	27/02/13 04:48:26	27/02/13 04:48:26
WindowsImageBackup	20/05/16 20:12:03	20/05/16 20:12:03	20/05/16 20:12:03	20/05/16 20:12:03
{34c137b2-8056-11e2-bebf-d0df9a3dfe1b}{3808876b-c176-4e48-b7ae-04046e6cc752}	26/02/13 20:56:14	26/02/13 20:56:14	20/05/16 20:12:26	20/05/16 20:12:26
{3808876b-c176-4e48-b7ae-04046e6cc752}	26/02/13 20:56:14	26/02/13 20:56:14	26/02/13 20:56:14	26/02/13 20:56:14
{406df1f4-1e83-11e6-a28a-000c296e6e9e}{3808876b-c176-4e48-b7ae-04046e6cc752}	20/05/16 20:12:23	20/05/16 20:12:23	28/05/16 07:00:06	28/05/16 07:00:06
{406df341-1e83-11e6-a28a-000c296e6e9e}{3808876b-c176-4e48-b7ae-04046e6cc752}	28/05/16 07:00:04	28/05/16 07:00:04	05/06/16 07:00:04	05/06/16 07:00:04
{406df3ea-1e83-11e6-a28a-000c296e6e9e}{3808876b-c176-4e48-b7ae-04046e6cc752}	05/06/16 07:00:02	05/06/16 07:00:02	13/06/16 07:00:05	13/06/16 07:00:05
{406df499-1e83-11e6-a28a-000c296e6e9e}{3808876b-c176-4e48-b7ae-04046e6cc752}	13/06/16 07:00:03	13/06/16 07:00:03	15/06/16 11:16:25	15/06/16 11:16:25
{406df4ef-1e83-11e6-a28a-000c296e6e9e}{3808876b-c176-4e48-b7ae-04046e6cc752}	15/06/16 11:16:23	15/06/16 11:16:23	15/06/16 11:16:23	15/06/16 11:16:23

Figure 11: Volume Shadow Copy Normal Situation

A volume shadow copy found out of sequence may indicate backdating of the system clock. Figure 12 contains 16 volume shadow copies created from 12/22/2015 to 6/9/2016 and sorted by the file created time. The volume shadow copies created within a close time range have similar names. These are grouped using different colors. However, the dispersed volume shadow copy created on 4/20/2016 16:30 does not have a similar name as either "orange group" or "blue group" nearby. It has a similar name as the "yellow group" which means this volume shadow copy should have been created after the "blue group." This volume shadow copy was created with a backdated system clock.

Sort ↓

Name	File Created
{58c5b5db-a53d-11e5-a5c0-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	22/12/2015 11:01
{58c5b716-a53d-11e5-a5c0-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	30/12/2015 00:00
{58c5bd4d-a53d-11e5-a5c0-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	06/01/2016 00:00
{58c5bdc6-a53d-11e5-a5c0-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	07/01/2016 17:36
{58c5be2a-a53d-11e5-a5c0-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	08/01/2016 11:17
{c6f59c3b-fd89-11e5-829c-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	09/04/2016 03:37
{c6f5b48c-fd89-11e5-829c-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	17/04/2016 00:00
{c6f5b50f-fd89-11e5-829c-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	18/04/2016 12:28
{d329356a-1bf1-11e6-bda1-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	20/04/2016 16:30
{8b40e22c-06c7-11e6-af47-40167eb4185a}{3808876b-c176-4e48-b7ae-04046e6cc752}	26/04/2016 00:00
{8b40e318-06c7-11e6-af47-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	03/05/2016 00:00
{8b40e41b-06c7-11e6-af47-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	10/05/2016 00:00
{d329348c-1bf1-11e6-bda1-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	17/05/2016 14:17
{d329361d-1bf1-11e6-bda1-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	25/05/2016 00:00
{d32936ef-1bf1-11e6-bda1-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	02/06/2016 00:00
{d32937aa-1bf1-11e6-bda1-54271e61f666}{3808876b-c176-4e48-b7ae-04046e6cc752}	09/06/2016 00:00

The dispersed VSC does not belong to any group nearby, but has similar name as "yellow group"

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

Figure 12: Volume Shadow Copy System Backdating

3.1.7. $Stdinfo and $Filename Timestamps

The modified, created, and accessed timestamps shown in Windows Explorer are stored as $Stdinfo attributes. Time modification tools, such as Timestamp, can easily change the $Stdinfo attributes. In Figure 13, Timestamp is used to backdate the timestamps from 6/17/2016 to 5/17/2016.

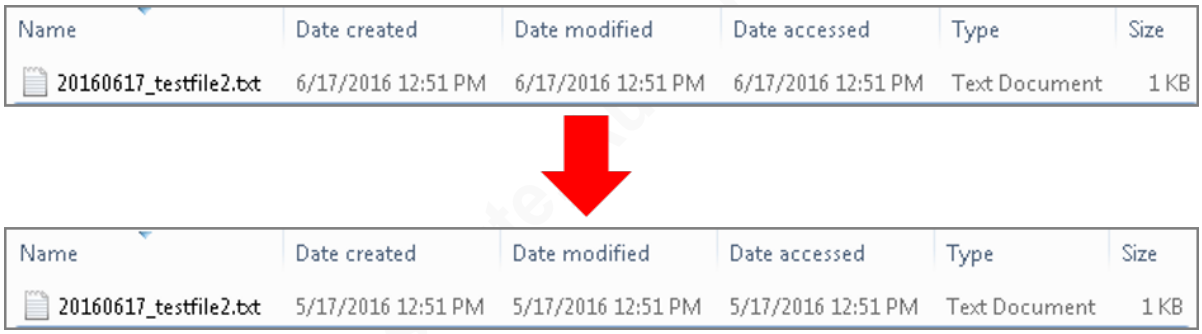
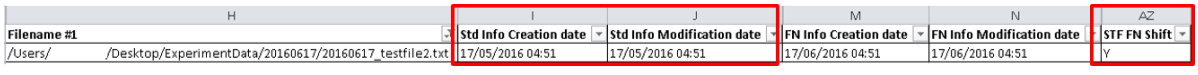


Figure 13: Timestamp Modification of $Stdinfo

Apart from $Stdinfo attributes, there are also $Filename attributes which contain the timestamps. Tools like Timestomp can reset the $Stdinfo attributes for a file to an arbitrary time, but not the $Filename attributes. Therefore, $Filename attributes contain the real timestamps, while $Stdinfo attributes contain the modified timestamps. By comparing $Stdinfo timestamps and $Filename timestamps using analyzeMFT.py script (Kovar, 2016), if $Stdinfo timestamps go before $Filename timestamps, the timestamps of the file may have been backdated. Figure 14 is the output for the example file from the analyzeMFT.py script, which indicates backdating of the $Stdinfo timestamps in the archives.



H	I	J	M	N	AZ
Filename #1	Std Info Creation date	Std Info Modification date	FN Info Creation date	FN Info Modification date	STF FN Shift
/Users/ /Desktop/ExperimentData/20160617/20160617_testfile2.txt	17/05/2016 04:51	17/05/2016 04:51	17/06/2016 04:51	17/06/2016 04:51	Y

Figure 14: Backdating of $Stdinfo Timestamps

3.1.8. CBS Log

The CBS.log, located at C:\Windows\Logs\CBS\CBS.log, is updated when the System File Checker or Windows Modules Installer conducts certain operations. The System File Checker SFC.exe writes the details of each verification and each repair

© 2017 The SANS Institute Author retains full rights.

process to CBS.log. The Windows Modules Installer also writes to this log when installing optional features, updates, and service packs. The latest record is written at the end of the log. The record sequence should be consistent with the time sequence, If not, backdating of the system clock is indicated. Although this file is not updated as regularly as WindowsUpdate.log, it can be still considered as an indication for system clock backdating.

3.2. Application Artifacts

3.2.1. Antivirus Update Log

When antivirus (AV) software is installed, we can find the trace of system clock change in the AV update log. For Symantec, the LiveUpdate will record all activities in "C:\ProgramData\Symantec\LiveUpdate\Log.LiveUpdate" every hour. LiveUpdate will write the time according to the system clock. The latest record is written at the end of the log file. Normally, the time of the records will increase when these records are created (Figure 15).

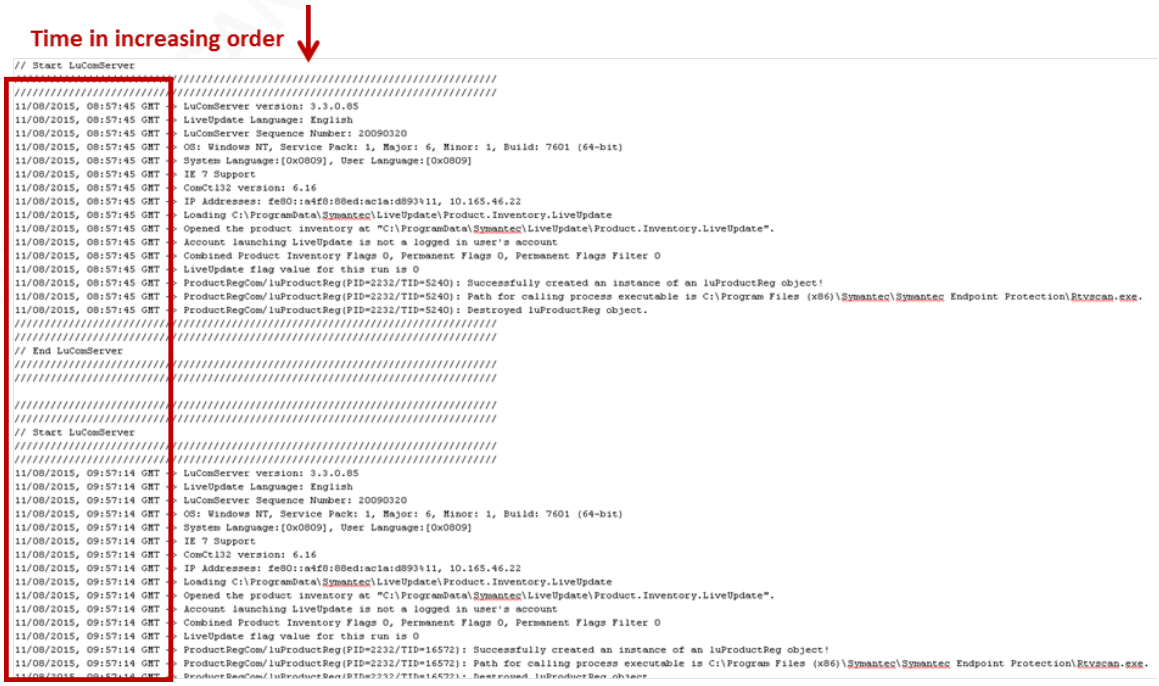


Figure 15: AV Log Normal Situation

© 2017 The SANS Institute Author retains full rights.

If the time sequence of the records decreases, backdating of the system clock during this period may have occurred. In Figure 16, we can tell the system clock has been backdated one day between 8/11/2015 10:57 to 8/11/2015 11:57.

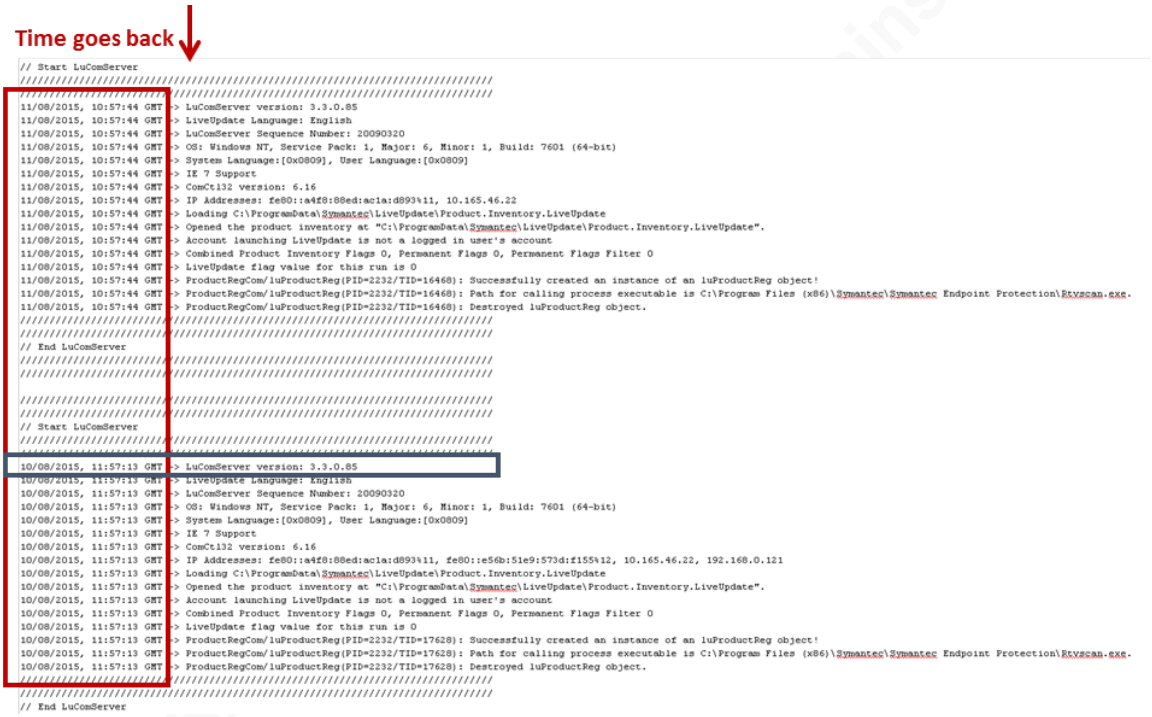


Figure 16: AV Log System Backdating

3.2.2. Google Drive Sync Log

Installations of Google Drive result in a sync log being installed on the computer. For a Windows 7 system, this is located at %APPDATA%\Local\Google\Drive\sync_log.log. Under normal situation, the latest record is at the end of the log (Figure 17).

© 2017 The SANS Institute Author retains full rights.

Figure 17: Google Drive Log Normal Situation

As shown in Figure 18, the time order of the records not continuously increasing indicates backdating of the system clock.

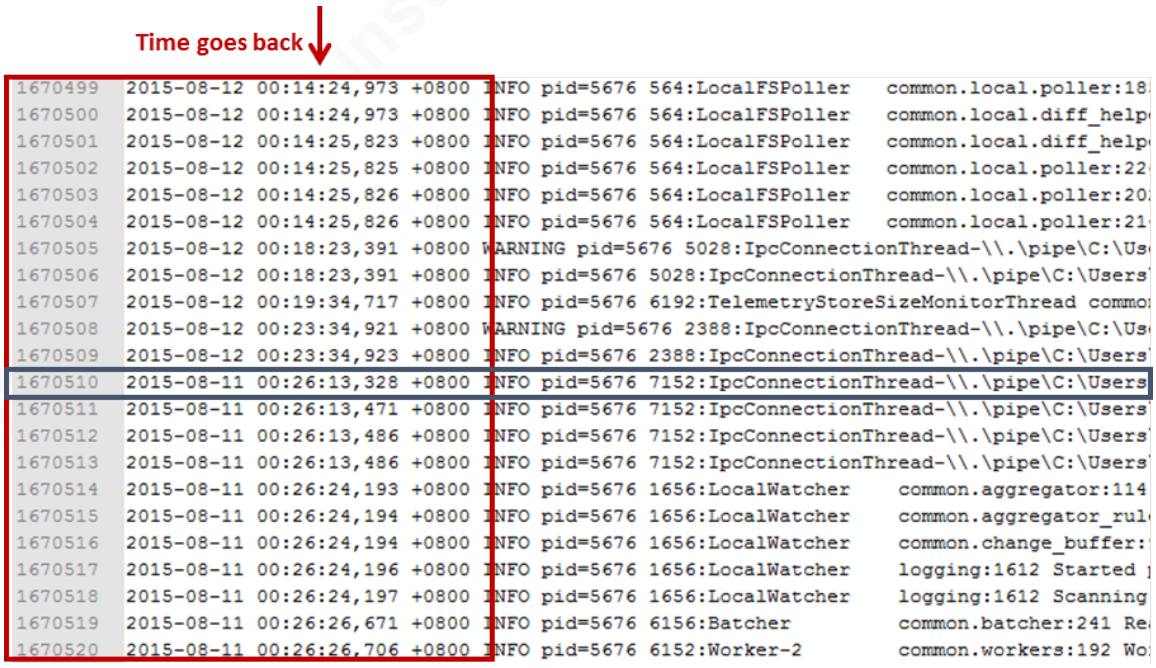


Figure 18: Google Drive Log System Backdating

3.2.3. Vmware-usbarb-n Log

If VMware is used, the log for VMware USB Arbitration Service, vmware-usbarb-n.log, is located under C:\Windows\Temp\vmware-SYSTEM. The connection activity of the VM client is recorded in this log. Again, the latest record is written at the end of each log.

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

In the case where the time sequence of records goes backward, backdating of the system clock can be inferred. Figure 19 shows an example where backdating of the system clock one day has occurred.

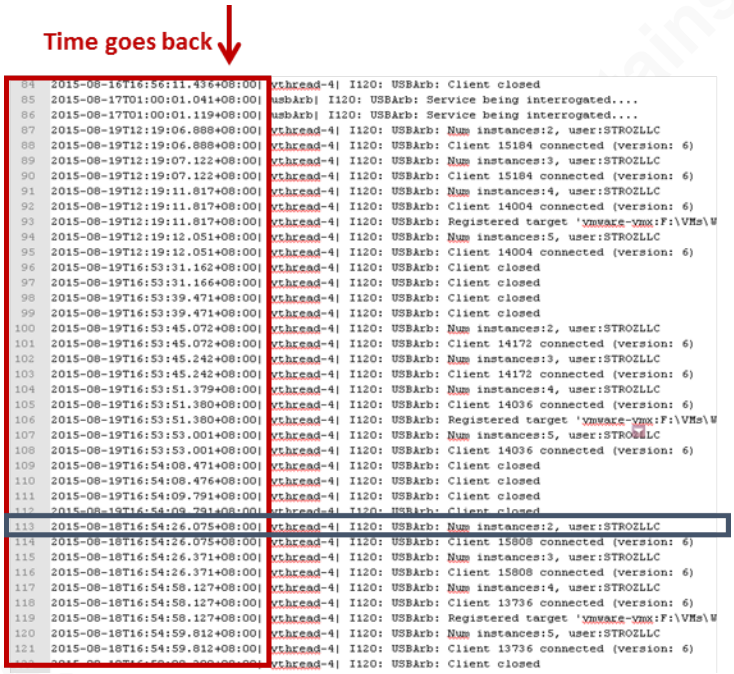


Figure 19: VMware System Backdating

3.3. Internet Artifacts

3.3.1. Internet History

Browser history for Chrome is contained in a SQLite database located at %APPDATA%\Local\Google\Chrome\User Data\Default\History. Figure 20 shows that, in the table "visits," the column "id" will be continuously increasing with the writing of each new record. The column "visit_time" (local system time) should be in increasing sequence consistent with column "id." Small discrepancies between column "id" and "visit_time" are typical. However, significant differences such as on the order of one day may indicate backdating of the system clock.

© 2017 The SANS Institute Author retains full rights.

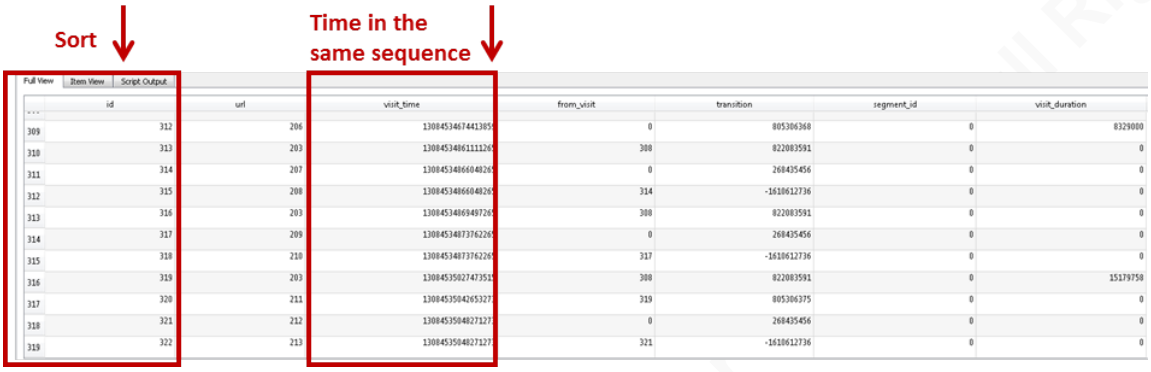
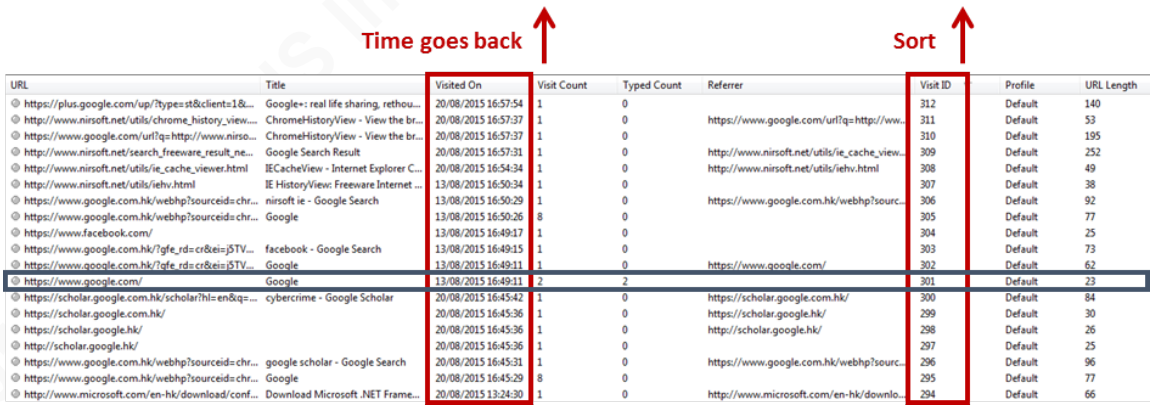


Figure 20: Chrome History Normal Situation

To better view, the history data, Nirsoft's ChromeHistoryView v1.22 (Nirsoft, 2011) was used to parse the database. In the following example, column "Visit ID" and "Visited On" are not consistent in a sequence that indicates the system clock has been backdated seven days on 8/20/2015.

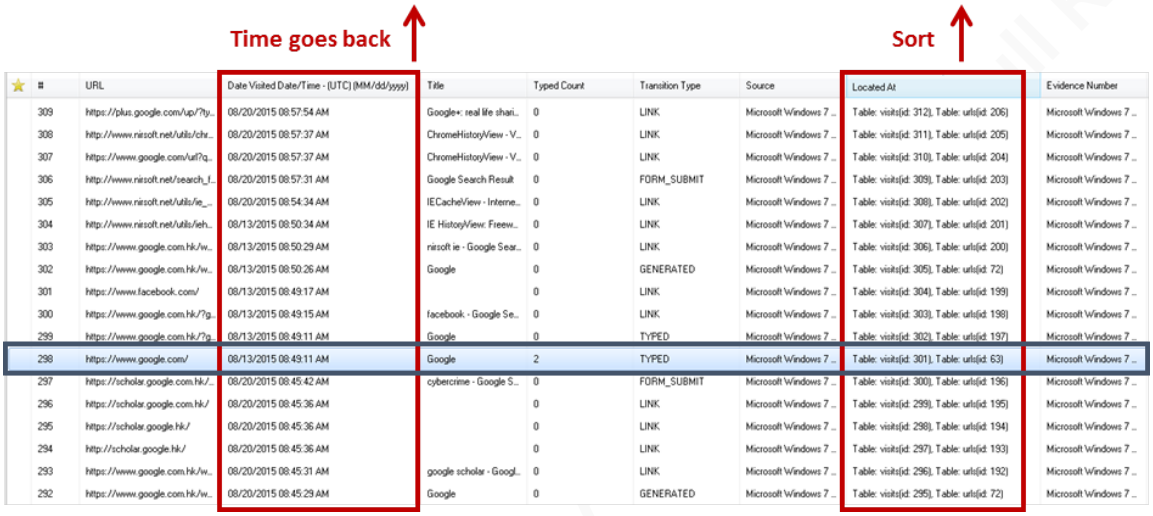


URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit ID	Profile	URL Length
https://plus.google.com/up/?type=st&client=1&...	Google+: real life sharing, rethou...	20/08/2015 16:57:54	1	0		312	Default	140
http://www.nirsoft.net/utils/chrome_history_view....	ChromeHistoryView - View the br...	20/08/2015 16:57:37	1	0	https://www.google.com/url?q=http://ww...	311	Default	53
https://www.google.com/url?q=http://www.nirso...	ChromeHistoryView - View the br...	20/08/2015 16:57:37	1	0		310	Default	195
http://www.nirsoft.net/search_freeware_result_ne...	Google Search Result	20/08/2015 16:57:31	1	0	http://www.nirsoft.net/utils/ie_cache_view...	309	Default	252
http://www.nirsoft.net/utils/ie_cache_viewer.html	IECacheView - Internet Explorer C...	20/08/2015 16:54:34	1	0	http://www.nirsoft.net/utils/iehv.html	308	Default	49
http://www.nirsoft.net/utils/iehv.html	IE HistoryView: Freeware Internet ...	13/08/2015 16:50:34	1	0		307	Default	38
https://www.google.com.hk/webhp?sourceid=chr...	nirsoft ie - Google Search	13/08/2015 16:50:29	1	0	https://www.google.com.hk/webhp?sourc...	306	Default	92
https://www.google.com.hk/webhp?sourceid=chr...	Google	13/08/2015 16:50:26	8	0		305	Default	77
https://www.facebook.com/		13/08/2015 16:49:17	1	0		304	Default	25
https://www.google.com.hk/?gfe_rd=cr&ei=j5TV...	facebook - Google Search	13/08/2015 16:49:15	1	0		303	Default	73
https://www.google.com.hk/?gfe_rd=cr&ei=j5TV...	Google	13/08/2015 16:49:11	1	0	https://www.google.com/	302	Default	62
https://www.google.com/	Google	13/08/2015 16:49:11	2	2		301	Default	23
https://scholar.google.com.hk/scholar?hl=en&q=...	cybercrime - Google Scholar	20/08/2015 16:45:42	1	0	https://scholar.google.com.hk/	300	Default	84
https://scholar.google.com.hk/		20/08/2015 16:45:36	1	0	https://scholar.google.hk/	299	Default	30
https://scholar.google.hk/		20/08/2015 16:45:36	1	0	http://scholar.google.hk/	298	Default	26
http://scholar.google.hk/		20/08/2015 16:45:36	1	0		297	Default	25
https://www.google.com.hk/webhp?sourceid=chr...	google scholar - Google Search	20/08/2015 16:45:31	1	0	https://www.google.com.hk/webhp?sourc...	296	Default	96
https://www.google.com.hk/webhp?sourceid=chr...	Google	20/08/2015 16:45:29	8	0		295	Default	77
http://www.microsoft.com/en-hk/download/conf...	Download Microsoft .NET Frame...	20/08/2015 13:24:30	1	0	http://www.microsoft.com/en-hk/downlo...	294	Default	66

IEF also can generate the Internet history report. Figure 22 is the "Chrome Web Visits" generated by IEF, sorted by column "Located At" (sort by table "visits," field "id"). The inconsistency of sequence in column "Date Visited Date/Time" indicates the system clock backdate. Note in IEF, "Chrome Web History" is according to table "urls" that the same URL is recorded once with its last visit date/time, "Chrome Web Visits" is according to table "visits" that will record every visit with the visit date/time.

Xiaoxi Fan, xfan@strozfriedberg.com

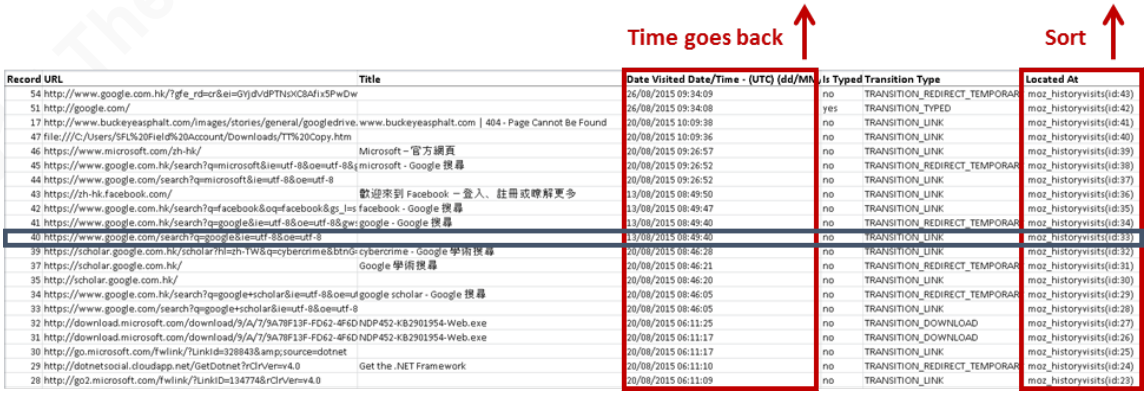
© 2017 The SANS Institute Author retains full rights.



#	URL	Date Visited Date/Time - (UTC) (MM/dd/yyyy)	Title	Typed Count	Transition Type	Source	Located At	Evidence Number
309	https://plus.google.com/up/?ty...	08/20/2015 08:57:54 AM	Google+: real life shari...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 312), Table: urls(id: 206)	Microsoft Windows 7 ...
308	http://www.nirsoft.net/utils/chr...	08/20/2015 08:57:37 AM	ChromeHistoryView - V...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 311), Table: urls(id: 205)	Microsoft Windows 7 ...
307	https://www.google.com/url?q...	08/20/2015 08:57:37 AM	ChromeHistoryView - V...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 310), Table: urls(id: 204)	Microsoft Windows 7 ...
306	http://www.nirsoft.net/search_f...	08/20/2015 08:57:31 AM	Google Search Result	0	FORM_SUBMIT	Microsoft Windows 7 ...	Table: visits(id: 309), Table: urls(id: 203)	Microsoft Windows 7 ...
305	http://www.nirsoft.net/utils/ie_...	08/20/2015 08:54:34 AM	IECacheView - Interne...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 308), Table: urls(id: 202)	Microsoft Windows 7 ...
304	http://www.nirsoft.net/utils/ieh...	08/13/2015 08:50:34 AM	IE HistoryView: Freew...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 307), Table: urls(id: 201)	Microsoft Windows 7 ...
303	https://www.google.com.hk/w...	08/13/2015 08:50:29 AM	nirsoft ie - Google Sear...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 306), Table: urls(id: 200)	Microsoft Windows 7 ...
302	https://www.google.com.hk/w...	08/13/2015 08:50:26 AM	Google	0	GENERATED	Microsoft Windows 7 ...	Table: visits(id: 305), Table: urls(id: 72)	Microsoft Windows 7 ...
301	https://www.facebook.com/	08/13/2015 08:49:17 AM		0	LINK	Microsoft Windows 7 ...	Table: visits(id: 304), Table: urls(id: 199)	Microsoft Windows 7 ...
300	https://www.google.com.hk/?g...	08/13/2015 08:49:15 AM	facebook - Google Se...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 303), Table: urls(id: 198)	Microsoft Windows 7 ...
299	https://www.google.com.hk/?g...	08/13/2015 08:49:11 AM	Google	0	TYPED	Microsoft Windows 7 ...	Table: visits(id: 302), Table: urls(id: 197)	Microsoft Windows 7 ...
298	https://www.google.com/	08/13/2015 08:49:11 AM	Google	2	TYPED	Microsoft Windows 7 ...	Table: visits(id: 301), Table: urls(id: 63)	Microsoft Windows 7 ...
297	https://scholar.google.com.hk/...	08/20/2015 08:45:42 AM	cybercrime - Google S...	0	FORM_SUBMIT	Microsoft Windows 7 ...	Table: visits(id: 300), Table: urls(id: 196)	Microsoft Windows 7 ...
296	https://scholar.google.com.hk/	08/20/2015 08:45:36 AM		0	LINK	Microsoft Windows 7 ...	Table: visits(id: 299), Table: urls(id: 195)	Microsoft Windows 7 ...
295	https://scholar.google.hk/	08/20/2015 08:45:36 AM		0	LINK	Microsoft Windows 7 ...	Table: visits(id: 298), Table: urls(id: 194)	Microsoft Windows 7 ...
294	http://scholar.google.hk/	08/20/2015 08:45:36 AM		0	LINK	Microsoft Windows 7 ...	Table: visits(id: 297), Table: urls(id: 193)	Microsoft Windows 7 ...
293	https://www.google.com.hk/w...	08/20/2015 08:45:31 AM	google scholar - Googl...	0	LINK	Microsoft Windows 7 ...	Table: visits(id: 296), Table: urls(id: 192)	Microsoft Windows 7 ...
292	https://www.google.com.hk/w...	08/20/2015 08:45:29 AM	Google	0	GENERATED	Microsoft Windows 7 ...	Table: visits(id: 295), Table: urls(id: 72)	Microsoft Windows 7 ...

Figure 22: Chrome Web Visits

Firefox presents a similar approach as Chrome. The history of Firefox is located at %APPDATA%\Roaming\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite. After using IEF to export "Firefox Web Visits," sort it by table "moz_historyvisits" & field "id," compare the sequence in column "Date Visited Date/Time" to detect any inconsistency. The following example has a backdated system clock on 8/20/2015.



Record URL	Title	Date Visited Date/Time - (UTC) (dd/MM/	Is Typed	Transition Type	Located At
54 http://www.google.com.hk/?gfe_rd=cr&ei=GYjdVdPTNsXC8Afix5PwDw		26/08/2015 09:34:09	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:43)
51 http://google.com/		26/08/2015 09:34:08	yes	TRANSITION_TYPED	moz_historyvisits(id:42)
17 http://www.buckeyeasphalt.com/images/stories/general/googledrive...	www.buckeyeasphalt.com | 404 - Page Cannot Be Found	20/08/2015 10:09:38	no	TRANSITION_LINK	moz_historyvisits(id:41)
47 file:///C:/Users/SFL%20Field%20Account/Downloads/TT%20Copy.htm		20/08/2015 10:09:36	no	TRANSITION_LINK	moz_historyvisits(id:40)
46 https://www.microsoft.com/zh-hk/	Microsoft – 官方網頁	20/08/2015 09:26:57	no	TRANSITION_LINK	moz_historyvisits(id:39)
45 https://www.google.com.hk/search?q=microsoft&ie=utf-8&oe=utf-8&...	microsoft - Google 搜尋	20/08/2015 09:26:52	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:38)
44 https://www.google.com/search?q=microsoft&ie=utf-8&oe=utf-8		20/08/2015 09:26:52	no	TRANSITION_LINK	moz_historyvisits(id:37)
43 https://zh-hk.facebook.com/	歡迎來到 Facebook – 登入、註冊或瞭解更多	13/08/2015 08:49:50	no	TRANSITION_LINK	moz_historyvisits(id:36)
42 https://www.google.com.hk/search?q=facebook&oq=facebook&gs_l=s...	facebook - Google 搜尋	13/08/2015 08:49:47	no	TRANSITION_LINK	moz_historyvisits(id:35)
41 https://www.google.com.hk/search?q=google&ie=utf-8&oe=utf-8&gw=...	google - Google 搜尋	13/08/2015 08:49:40	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:34)
40 https://www.google.com/search?q=google&ie=utf-8&oe=utf-8		13/08/2015 08:49:40	no	TRANSITION_LINK	moz_historyvisits(id:33)
39 https://scholar.google.com.hk/scholar?hl=zh-TW&q=cybercrime&btnG=...	cybercrime - Google 學術搜尋	20/08/2015 08:46:28	no	TRANSITION_LINK	moz_historyvisits(id:32)
37 https://scholar.google.com.hk/	Google 學術搜尋	20/08/2015 08:46:21	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:31)
35 http://scholar.google.com.hk/		20/08/2015 08:46:20	no	TRANSITION_LINK	moz_historyvisits(id:30)
34 https://www.google.com.hk/search?q=google+scholar&ie=utf-8&oe=ut...	google scholar - Google 搜尋	20/08/2015 08:46:05	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:29)
33 https://www.google.com/search?q=google+scholar&ie=utf-8&oe=utf-8		20/08/2015 08:46:05	no	TRANSITION_LINK	moz_historyvisits(id:28)
32 http://download.microsoft.com/download/9/A/7/9A78F13F-FD62-4F6D...	NDP452-KB2901954-Web.exe	20/08/2015 06:11:25	no	TRANSITION_DOWNLOAD	moz_historyvisits(id:27)
31 http://download.microsoft.com/download/9/A/7/9A78F13F-FD62-4F6D...	NDP452-KB2901954-Web.exe	20/08/2015 06:11:17	no	TRANSITION_DOWNLOAD	moz_historyvisits(id:26)
30 http://go.microsoft.com/fwlink/?LinkId=328843&source=dotnet		20/08/2015 06:11:17	no	TRANSITION_LINK	moz_historyvisits(id:25)
29 http://dotnetsocial.cloudapp.net/GetDotnet?rClrVer=v4.0	Get the .NET Framework	20/08/2015 06:11:10	no	TRANSITION_REDIRECT_TEMPORAR	moz_historyvisits(id:24)
28 http://go2.microsoft.com/fwlink/?LinkID=134774&rClrVer=v4.0		20/08/2015 06:11:09	no	TRANSITION_LINK	moz_historyvisits(id:23)

Figure 23: Firefox System Backdating

3.3.2. Internet Download

Chrome download history is also stored in %APPDATA%\Local\Google\Chrome\User Data\Default\History. In table "downloads," the column "id" is continuously increasing when adding a new download record. Each

© 2017 The SANS Institute Author retains full rights.

record represents a download. The column "start time date/time" is the time when the download started, the time obtained from local system clock time.

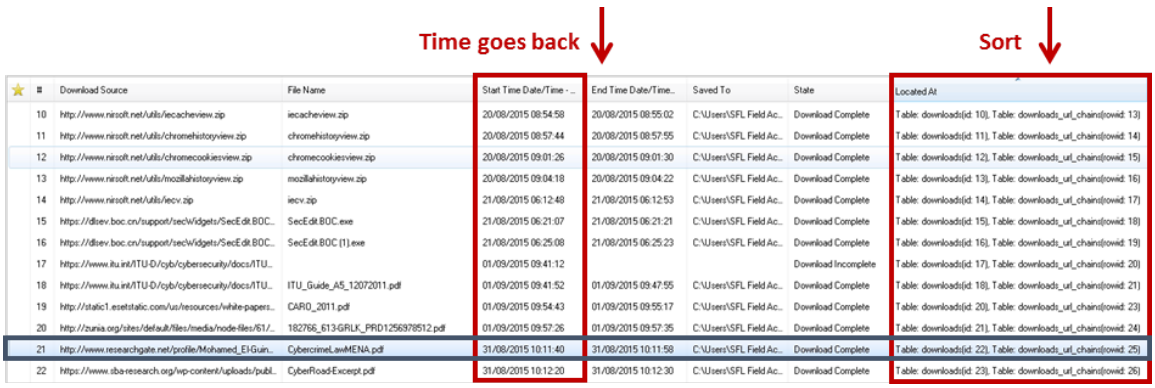
We performed a few tests to observe the behaviors of Chrome. If a download is paused and resumed again, the "start time" is the time when the download was firstly started and does not update to the resume time.

If a download is canceled and then restarted from the download window, there will be two records in download history. The "start time" of the first record is the time when the download first started. The "start time" of the second record is the time when the download restarted.

A download removed from the download list also deletes the record from table "downloads." In column "id," if there is a gap in the middle from removing a record from the list, the id number will not get used.

Therefore, the column "id" indicates the sequence of download actions, and the column "start time date/time" should be consistent with this sequence. When "id" increases, "start time date/time" should increase. Otherwise, backdating of the system clock may have occurred.

In the example, IEF is used to parse "Chrome Downloads," after sorting the records according to table "downloads" and field "id," we can check column "start time date/time" and find the system clock backdate at line 21.



#	Download Source	File Name	Start Time Date/Time - ...	End Time Date/Time...	Saved To	State	Located At
10	http://www.nirsoft.net/utils/iecacheview.zip	iecacheview.zip	20/08/2015 08:54:58	20/08/2015 08:55:02	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 10), Table: downloads_url_chains(rowid: 13)
11	http://www.nirsoft.net/utils/chromehistoryview.zip	chromehistoryview.zip	20/08/2015 08:57:44	20/08/2015 08:57:55	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 11), Table: downloads_url_chains(rowid: 14)
12	http://www.nirsoft.net/utils/chromecookiesview.zip	chromecookiesview.zip	20/08/2015 09:01:26	20/08/2015 09:01:30	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 12), Table: downloads_url_chains(rowid: 15)
13	http://www.nirsoft.net/utils/mozillahistoryview.zip	mozillahistoryview.zip	20/08/2015 09:04:18	20/08/2015 09:04:22	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 13), Table: downloads_url_chains(rowid: 16)
14	http://www.nirsoft.net/utils/iecv.zip	iecv.zip	21/08/2015 06:12:48	21/08/2015 06:12:53	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 14), Table: downloads_url_chains(rowid: 17)
15	https://dlsev.boc.cn/support/secWidgets/SecEdit.BOC...	SecEdit.BOC.exe	21/08/2015 06:21:07	21/08/2015 06:21:21	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 15), Table: downloads_url_chains(rowid: 18)
16	https://dlsev.boc.cn/support/secWidgets/SecEdit.BOC...	SecEdit.BOC (1).exe	21/08/2015 06:25:08	21/08/2015 06:25:23	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 16), Table: downloads_url_chains(rowid: 19)
17	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU...		01/09/2015 09:41:12			Download Incomplete	Table: downloads(id: 17), Table: downloads_url_chains(rowid: 20)
18	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU...	ITU_Guide_A5_12072011.pdf	01/09/2015 09:41:52	01/09/2015 09:47:55	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 18), Table: downloads_url_chains(rowid: 21)
19	http://static1.esetstatic.com/us/resources/white-papers...	CARO_2011.pdf	01/09/2015 09:54:43	01/09/2015 09:55:17	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 20), Table: downloads_url_chains(rowid: 23)
20	http://zurich.org/sites/default/files/media/node-files/61/...	182766_613-GRLK_PRD1256978512.pdf	01/09/2015 09:57:26	01/09/2015 09:57:35	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 21), Table: downloads_url_chains(rowid: 24)
21	http://www.researchgate.net/profile/Mohamed_El-Guin...	CybercrimeLawMENA.pdf	31/08/2015 10:11:40	31/08/2015 10:11:58	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 22), Table: downloads_url_chains(rowid: 25)
22	https://www.sba-research.org/wp-content/uploads/publ...	CyberRoad-Excerpt.pdf	31/08/2015 10:12:20	31/08/2015 10:12:30	C:\Users\SFL Field Ac...	Download Complete	Table: downloads(id: 23), Table: downloads_url_chains(rowid: 26)

Figure 24: Chrome Downloads System Backdating

For Firefox, download history is included in table "moz_annos" of %APPDATA%\Roaming\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite. Since

© 2017 The SANS Institute Author retains full rights.

IEF does not parse the "start time," we need to look at the history file. In table "moz_annos," filter column "anno_attribute_id" with all download related attributes, then compare the sequence in column "id" and column "dateAdded." The inconsistency in these two columns indicates system clock backdate.

3.3.3. Internet Cookie

A cookie may contain timestamps; some represent local system time, others the server side (Obsidian Forensics, 2013). Server-side timestamps include cookie creation time and cookie last access time. Backdating of the system clock can be determined by comparing these timestamps. Since the server-side time extracted from the cookie is the actual time, it will be quite different from the cookie creation/last access time generated locally. A small difference like a few seconds between the server-side timestamp and cookie creation/last access time is reasonable, while significant difference like days or months demand attention.

In the following example, Firefox's cookies report is extracted using IEF. By comparing the server-side timestamp, highlighted in column "value," and the cookie creation/last access time (column "creation date/time" or "last accessed date/time"), we can tell whether the system clock is correct during that period. In the example, the server-side timestamp is translated (column "server-side timestamp"). We can see many popular websites contain server-side timestamps in the cookies, like Google, Twitter, Baidu, Wikipedia, LinkedIn, Sina Weibo, Microsoft, and Reddit.

Accessing a cookie for the second time if the server-side timestamp records the cookie creation time, then the server-side timestamp in the "value" will not change; while if the server-side timestamp records the cookie last access time, then the server-side timestamp in the "value" will update. Therefore, we can test to determine whether a server-side timestamp is cookie creation time or cookie last access time so that the server-side timestamp can be compared to the corresponding locally generated cookie time. The server-side timestamps in the example have been tested and noted in column "server-side_creation or last access," then the translated server-side timestamp is compared to the corresponding cookie creation/last access time to detect system clock change. In the

© 2017 The SANS Institute Author retains full rights.

example, the system clock has been backdated to 8/19/2015 on 8/26/2015 and backdated to 8/30/2015 on 8/31/2015.

Firefox Cookies

Name	Value	Server-Side Timestamp	Server-Side_Creation or Last Access	Last Accessed Date/Time	Creation Date/Time	Host
PREF	ID=1111111111111111:TM=1440581728:LM=1440581728:V=1:S=fG9uONyemsVK41_w	26/08/2015 09:35	Creation	30/08/2015 02:25:35	19/08/2015 09:35:19	.google.com
PREF	ID=1111111111111111:FF=0:TM=1440581729:LM=1440581729:V=1:S=yJuMubl_XYXbxM29	26/08/2015 09:35	Creation	30/08/2015 02:25:35	19/08/2015 09:35:20	.google.com.hk
guest_id	v1%3A144058179343789056	26/08/2015 09:36	Creation	30/08/2015 02:25:54	19/08/2015 09:36:24	.twitter.com
PREF	ID=1111111111111111:FF=0:TM=1440581802:LM=1440581802:V=1:S=8y4KE5bkHo4p3z-B	26/08/2015 09:36	Creation	30/08/2015 02:25:35	19/08/2015 09:36:33	.google.com
id	227dd9c3300400005||t=1440581849|et=730|cs=002213fd48247234132b6dbb82	26/08/2015 09:37	Creation	30/08/2015 02:25:35	19/08/2015 09:37:20	.doubleclick.net
PSTM	1440581870	26/08/2015 09:37	Creation	30/08/2015 02:15:57	19/08/2015 09:37:41	.baidu.com
lr_uid	3.1440582007383.14597849267309222787	26/08/2015 09:40	Creation	30/08/2015 09:39:58	19/08/2015 09:39:58	.liverail.com
i	9aa5eedd-3fa1-4ab6-ae59-58a5e3ef73fa|1440582007	26/08/2015 09:40	Creation	30/08/2015 02:25:59	19/08/2015 09:39:58	.openx.net
WMF-Last-Access	26-Aug-2015	26/08/2015	Last Access	19/08/2015 09:40:02	19/08/2015 09:40:02	wikipedia.com
WMF-Last-Access	31-Aug-2015	31/08/2015	Last Access	30/08/2015 02:17:17	19/08/2015 09:40:03	www.wikipedia.org
atpsida	ec1a735393a5236aee8af946_1440987595	31/08/2015 02:19	Last Access	30/08/2015 02:19:43	19/08/2015 09:42:05	.mmstat.com
aimx	xHdkDtS5OnYCAdIFqkJFbFct_1440987529	31/08/2015 02:18	Last Access	30/08/2015 02:19:52	19/08/2015 09:42:07	.mmstat.com
SINAGLOBAL	210.5.170.66_1440582194.351309	26/08/2015 09:43	Creation	30/08/2015 02:19:32	19/08/2015 09:43:05	.sina.com.cn
mt_mop	4:1440987625|10:1440987398	31/08/2015 02:20	Last Access	30/08/2015 02:20:13	19/08/2015 09:43:48	.mathtag.com
__cfduid	d35f6222917a51bd1b8363273a6de94ca1440582298	26/08/2015 09:44	Creation	30/08/2015 02:21:06	19/08/2015 09:44:49	.reddit.com
MC1	GUID=539a6bc71815124e84169ee3222f026b&HASH=c76b&LV=201508&V=4&LU=1440582714836	26/08/2015 09:51	Creation	30/08/2015 02:25:30	19/08/2015 09:51:45	.microsoft.com
pid	"v3:1440987315168223919547724"	31/08/2015 02:15	Creation	30/08/2015 02:25:54	30/08/2015 02:15:04	.twitter.com
UIDR	1440987368	31/08/2015 02:16	Creation	30/08/2015 02:20:27	30/08/2015 02:15:56	.scorecardresearch.com
lm	"31 Aug 2015 02:16:39 GMT"	31/08/2015 02:16	Creation	30/08/2015 02:25:59	30/08/2015 02:16:27	.rubiconproject.com
WMF-Last-Access	31-Aug-2015	31/08/2015	Last Access	30/08/2015 02:17:16	30/08/2015 02:17:16	wikipedia.org
WMF-Last-Access	31-Aug-2015	31/08/2015	Last Access	30/08/2015 02:17:19	30/08/2015 02:17:19	meta.wikimedia.org
WMF-Last-Access	31-Aug-2015	31/08/2015	Last Access	30/08/2015 02:17:59	30/08/2015 02:17:59	zh.wikipedia.org
WMF-Last-Access	31-Aug-2015	31/08/2015	Last Access	30/08/2015 02:18:02	30/08/2015 02:18:02	login.wikimedia.org
lidc	"b=LB74:g=218:u=1:i=1440987549:t=1441073949:s=AQGtkr9HHGaHd5Db8wWp2EO3832jzW3J"	31/08/2015 02:19	Creation	30/08/2015 02:18:57	30/08/2015 02:18:57	.linkedin.com
ATN	1.1440987674.4994051495126442100.AYK-2GQ6cOxhfnD86KE	31/08/2015 02:21	Creation	30/08/2015 02:25:56	30/08/2015 02:21:02	.admt.com

Figure 25: Cookie Analysis for System Backdating

3.3.4. Email

Like a cookie, an email header contains server generated timestamps (Table 1) which are the correct time(s) when the email is sent/received. If we find msg/eml email file on the computer, the MAC (modified, accessed, created) time of msg/eml file should not be earlier than the timestamp in the email header. Otherwise, one should be suspicious that backdating of the system clock may have occurred when the email is sent/received or tampering with the MAC time of the email has occurred.

Table 1: Email Header Analysis

*Received: from TEST1.PUBLIC (10.***.***.***) by TEST2.PUBLIC (10.***.***.***) with Microsoft SMTP Server (TLS) id 8.3.83.0; Wed, 12 Aug 2015 15:49:22 +0100*
*Received: from TEST3.PUBLIC ([fe80::****:****:****:****]) by TEST1.PUBLIC ([::1]) with mapi; Wed, 12 Aug 2015 10:49:52 -0400*
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: testing <testing@gmail.com>
Date: Wed, 12 Aug 2015 10:49:19 -0400
Subject: Testing Mail: 8.12.2015
Thread-Topic: Testing Mail: 8.12.2015
Thread-Index: AdDURlLGjGeqnJfUQriC0dWzJa570w==
Message-ID: <C196E3C30064894A9508503BB740B46E2803A2FB2A@TEST3.PUBLIC>
Accept-Language: en-US

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

```
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator:
<C196E3C30064894A9508503BB740B46E2803A2FB2A@TEST3.PUBLIC>
MIME-Version: 1.0
X-Auto-Response-Suppress: DR, OOF, AutoReply
To: Undisclosed recipients:;
Return-Path: testing@gmail.com
```

4. Conclusion

In this paper, we introduced various ways to determine whether backdating of or tampering with the system clock has occurred. We discussed three categories of artifacts related to the system, applications, and the Internet. We compared the patterns of timestamps in normal and backdating situations and determined that our hypothetical rules were proved to be correct.

We introduced how these artifacts maintain records, including estimating how many records can be expected in a given period so that the investigators can determine what objects would help in different situations. By applying these rules, we can tell if backdating or tampering has occurred.

For future work, the results from analyzing various artifacts will be combined to infer the details of backdating, e.g. when backdating of the system clock occurred, determining which timestamps to trust after backdating, and so forth

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.

References

Willassen S. Y. (2008). Methods for enhancement of timestamp evidence in digital investigations. Retrieved Dec 22, 2016, from http://www.cse.scu.edu/~tschwarz/COEN252_13/Papers/WillassenThesis.pdf

Farmer D. (2000). What are MACtimes? Retrieved Dec 22, 2016, from http://www.drdobbs.com/what-are-mactimes/184404275

Buchholz, F., & Tjaden, B. (2007). A brief study of time. Digital Investigation,4, 31-42.

Chow K. P., Law F. Y., Kwan M. Y., & Lai P. K. (2007). The rules of time on NTFS file system. In *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 71-85). IEEE.

Lee W. (2011). Rock around the clock. Retrieved Oct 31, 2016, from https://digital-forensics.sans.org/summit-archives/2011/2-rock-around-the-clock.pdf

Triforce (2014). Triforce ANJP free edition. Retrieved Oct 31, 2016, from https://www.gettriforce.com/product/anjp-free/

Oh J. (2013). NTFS log tracker. Retrieved Oct 31, 2016, from http://forensicinsight.org/wp-content/uploads/2013/06/F-INSIGHT-NTFS-Log-TrackerEnglish.pdf

Oh J. (2013). Advanced $UsnJrnl forensics. Retrieved Oct 31, 2016, from https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxmb3JlbnNpY25vdGV8Z3g6NzZhNzczNzE3ZDk0M2I1OA

Szynalski T. (2009). What you should know about volume shadow copy/system restore in Windows 7 & Vista. Retrieved Oct 31, 2016, from http://blog.szynalski.com/2009/11/volume-shadow-copy-system-restore/

Kovar D. (2016). AnalyzeMFT. Retrieved Oct 31, 2016, from https://github.com/dkovar/analyzeMFT

NirSoft. (2011). ChromeHistoryView v1.25. Retrieved Oct 31, 2016, from http://www.nirsoft.net/utils/chrome_history_view.html

Obsidian Forensics. (2013). Detecting clock changes using cookies. Retrieved Oct 31, 2016, from http://www.obsidianforensics.com/blog/detecting-clock-changes-using-cookies

Xiaoxi Fan, xfan@strozfriedberg.com

© 2017 The SANS Institute Author retains full rights.