Dynamic Time & Date Stamp Analysis

Michael C. Weil, Computer Forensic Examiner
Department Of Defense Computer Forensics Lab

Introduction

Dynamic time and date stamp analysis is a method for correlating times and dates contained within a file to the modified, accessed, and created/change of status (MAC) times of the file. This method can be used to standardize the apparent file MAC times to the actual time. The method will allow the examiner to derive the approximate actual system time.

Dynamic Time And Date Stamp Analysis In Practice

The dynamic time and date stamp methodology arose from an intrusion analysis. The time and date of intrusion identified by the intrusion detection system was March 10, 2001, 07:20 (GMT) or 1:20am (CST.) SUBJECT was located in the Central Standard Time zone, and the time of the system appeared to be consistent with the Central Standard Time Zone.

CMOS time and date review, and what you would expect to see upon analysis:

- The system time was 40 minutes slower than the actual time.
- The system date was 826 days slower than the actual date.
- MAC times of the files involved in the intrusion should have indicated December 5, 1998, 12:40am (CST) as the actual intrusion.

What was actually seen upon analysis:

- The MAC times of the files involved in the intrusion indicated that SUBJECT intruded on VICTIM systems on December 5, 1998, 1:00am (CST.)
- Analysis of the registry indicated the system time zone was set to Pacific Standard Time.
- Analysis of the Internet History file corroborated the MAC times by indicating that the intrusion occurred on December 4, 1998, 11:00pm (PST) or December 5, 1998, 1:00am (CST.)

The problem:

- Based on the difference between file MAC times corroborated by the Internet History file (December 5, 1998, at 1:00am) and the expected time and date of intrusion (December 5, 1998, at 12:40am,) SUBJECT's computer intruded on VICTIM system 20 minutes after the intrusion was alleged to have occurred.

A solution:

It was felt that external, independent sources of time could be used to standardize the system time and date. The Internet Cache folders were analyzed, and dynamic time and date stamps were identified within the body of HTML pages. The dynamic time and dates were correlated to the respective file's MAC times.

Results:

The MAC times were found to be 18 – 20 minutes slower than the time contained within the document. The MAC dates were found to be 826 days slower than the actual date. Based on the dynamic time and date correlation, SUBJECT's computer could be placed on the VICTIM computer at the exact time of the intrusion.

Conclusion:

The intrusion occurred on March 10, 2001 at 1:20 am (CST.) The MAC times were found to be 18 – 20 minutes slower than actual time. The MAC times of the files involed in the intrusion were December 5, 1998 at 1:00 am. If 826 days and 18 – 20 minutes were added to the MAC times, the result would be March 10, 1998 at 1:18 am to 1:20 am.

Cmos Limitations

The time and date within the CMOS has two limitations. The first limitation is the time and date standardization is a singular point in time. This singular point cannot account for time loss or gain in the CMOS time and date between occurrence of the crime, seizure and examination. The second limitation is if the SUBJECT changes the system time and date more than once, time and date standardization will be difficult, if not impossible.

Case For Dynamic Time And Date Stamp Analysis

Dynamic time and date stamp analysis does not rely on a singular point in time collection of the CMOS system time and date. The dynamic time and date stamp analysis relies on external, independent sources of time within a file and the MAC times gathered from the CMOS time and date at that singular point in time. The external, independent sources of time within a file can be correlated to the MAC times to yield an approximate actual system time and date. Further, when multiple sources of time are present, the reliability of approximate actual system time and date increases. In general, more independent sources of verification increase the reliability of the data because the external systems also utilize their individual system time and date. Therefore, the external systems are also subject to the same CMOS limitations. With multiple, independent, external sources of time and date, the external system's CMOS limitation can be minimized.

Methodology

(1) Identify files within the Internet Cache directory(ies) or other files that contain a time and/or date on the page. Identify, if possible, the time zone of the time and/or date.
(2) Preserve all files that contain a usable time and/or date stamp.
(3) Input relevant information into a spreadsheet. Relevant information would include the following: path, file name, MAC times, and observed time and/or date.

Example

Path	File Name	Modified	Accessed	Created	Observed
Internet Cache	File1.html	13:00	13:00	13:00	13:20
Internet Cache	File2.html	13:05	13:05	13:05	13:25
Internet Cache	File3.html	13:10	13:10	13:10	13:30
Internet Cache	File4.html	13:20	13:20	13:20	13:40
Internet Cache	File5.html	13:30	13:30	13:30	13:50
Internet Cache	File6.html	13:35	13:35	13:35	13:55
Internet Cache	File7.html	13:40	13:40	13:40	14:00
Internet Cache	File8.html	13:45	13:45	13:45	14:05

(4) Standardize all observed time and/or dates to the time zone the SUBJECT's computer is set to.

Example

Path	File Name	Modified	Accessed	Created	Observed	Observed Time Zone
Internet Cache	File1.html	13:00	13:00	13:00	13:20	UTC
Internet Cache	File2.html	13:05	13:05	13:05	13:25	UTC
Internet Cache	File3.html	13:10	13:10	13:10	13:30	UTC
Internet Cache	File4.html	13:20	13:20	13:20	13:40	UTC
Internet Cache	File5.html	13:30	13:30	13:30	13:50	UTC
Internet Cache	File6.html	13:35	13:35	13:35	13:55	UTC
Internet Cache	File7.html	13:40	13:40	13:40	14:00	UTC
Internet Cache	File8.html	13:45	13:45	13:45	14:05	UTC

(5) If the MAC time is greater than the observed time and/or date, then subtract the observed time and/or date from the MAC time. This indicates that the SUBJECT's computer is faster than the actual time.

Example: Since the modified, accessed, and created times are all equal, only one calculation was conducted for the difference between the MAC time and observed time.

Path	File Name	Modified	Accessed	Created	Observed	Observed Time Zone	Difference
Internet Cache	File1.html	13:00	13:00	13:00	12:01	UTC	0:59
Internet Cache	File2.html	13:05	13:05	13:05	12:05	UTC	1:00
Internet Cache	File3.html	13:10	13:10	13:10	12:12	UTC	0:58
Internet Cache	File4.html	13:20	13:20	13:20	12:21	UTC	0:59
Internet Cache	File5.html	13:30	13:30	13:30	12:30	UTC	1:00
Internet Cache	File6.html	13:35	13:35	13:35	12:36	UTC	0:59
Internet Cache	File7.html	13:40	13:40	13:40	12:42	UTC	0:58
Internet Cache	File8.html	13:45	13:45	13:45	12:45	UTC	1:00

(6) If the observed time and/or date is greater than the MAC time, then subtract the MAC time from the observed time and/or date. *Note (Change the font color to red. This step is necessary because most spreadsheet programs do not allow for negative times.) This indicates SUBJECT's computer is slower than the actual time.

Example: Since the modified, accessed, and created times are all equal, only one calculation was conducted for the difference between the MAC time and observed time.

Path	File Name	Modified	Accessed	Created	Observed	Observed Time Zone	Difference
Internet Cache	File11.html	13:00	13:00	13:00	13:21	UTC	0:21
Internet Cache	File12.html	13:05	13:05	13:05	13:25	UTC	0:20
Internet Cache	File13.html	13:10	13:10	13:10	13:32	UTC	0:22
Internet Cache	File14.html	13:20	13:20	13:20	13:41	UTC	0:21
Internet Cache	File15.html	13:30	13:30	13:30	13:50	UTC	0:20
Internet Cache	File16.html	13:35	13:35	13:35	13:57	UTC	0:22
Internet Cache	File17.html	13:40	13:40	13:40	14:00	UTC	0:20
Internet Cache	File18.html	13:45	13:45	13:45	14:05	UTC	0:20

(7) A range of date and times should now be calculated. If the range is minimal, an approximation can be used (i.e., the files was created between 12:25pm and 12:30pm.)

Example: As illustrated in the examples of Steps 5 and 6, the range in the time differences is minimal (2 minutes.) Therefore, the created time of file12.html was actually between 13:25 and 13:27 and not at 13:05.

(8) If there is wide variation in the time and/or date a conclusion may not be directly apparent without statistical models.

Results

In general, the created time and date should be sufficient for dynamic time and date stamp analysis. The modified time and date could be utilized if the document was

changed in the cache somehow, (e.g., the time and date changed on a subsequent visit.) This may be identified when the modified time and date are not equal to the created time and date. The accessed time and date may be a check on the created and modified time and date. It may be a check because the file may be accessed without access to the Internet.

Definitions

Time and date standardization – Adjusting a system time and date to reflect the actual time and date.

Static time and date stamp – A time and date stamp within a file that does not change when the file is accessed.

Dynamic time and date stamp – A time and date stamp within a file that changes when the file is accessed or accessed under specific conditions.

Dynamic time and date stamp analysis – Correlating times and dates contained within a file to the modified, accessed, and created (MAC) times of the file.

MAC times – Modified, Accessed, and Created times and dates. The MAC times utilize the system time when recording date and time. Modified time and date identifies the last time a file's contents were changed. Accessed time and date identifies the last time a file was accessed by a program or the user. Created time and date (in some operating systems referred to as Change in Status when changes are made to the location of the file or other factors,) identifies the time and date a file came to be present on a piece of computer media.

Approximate actual system time – An approximation of the time and date using either the time and date standardization or dynamic time and date stamp analysis.

Actual Time – The time and date by the examiner's watch.

System time – The time and date indicated in the CMOS. Also the time reflected in the MAC times.

Conclusion

The dynamic time and date stamp analysis can be used to identify the actual time and date of a system based on external sources of time and date. This can be extremely useful when the system time and date are not available or when the system time and date are altered one or more times.

About the Author

Mike Weil (Mike.Weil@dcfl.gov) is a Computer Forensic Examiner for the Department of Defense Computer Forensics Laboratory (DCFL.) He has been an examiner at DCFL since January 2000. In this position, Mr. Weil conducted media analysis in support of criminal and intrusion cases. Prior to his time at DCFL, Mr. Weil was the Senior Forensic Analysts for the Illinois Office of the Attorney General's Illinois Computer Crime Institute from 1998 to 2000. In this position, Mr. Weil provided computer forensic support for criminal investigations and training on computer investigations and forensics to law enforcement in the State of Illinois.

Mike Weil is a member of the National Institute of Justice's Technical Working Group for the Examination of Digital Evidence. He is also the Forensic Subcommittee Vice-Chairman for the Scientific Working Group on Digital Evidence, and he has served on the National Institute of Science and Technology's Computer Forensic Tool Testing and National Software Reference Library Steering Committee. Mr. Weil is currently pursuing a Masters of Business Administration from the University of Baltimore. He obtained a Bachelor of Science in Mathematics from Loyola University Chicago in 1998.