Timely: A Chain of Custody Data Visualizer

April Tanner
Department of Electrical and Computer Engineering and Computer Science
Jackson State University
Jackson, MS 39217, USA
april.l.tanner@jsums.edu

Jason Bruno
Department of Electrical and Computer Engineering and Computer Science
Jackson State University
Jackson, MS 39217, USA
j00733824@students.jsums.edu

***Abstract*—Digital forensics is a growing field with a high need for qualified professionals but a lack of people to fill this need. As a result, there is a need for the creation of forensic tools to help streamline this process and to allow those in the field and those that are breaking into the field to be able to learn and succeed in their respective careers. In the field, chain of custody reports are used to track and document changes in possession or ownership of evidence. While the written report is standard, timelines have been shown to be effective visualization tools in both organizing and displaying information, as well as educating those who use them. In this paper, we are proposing a web based interactive data visualization timeline that organizes the chain of custody and evidence information in an easy to understand and easily accessible interface.**

***Keywords* — digital forensics, chain of custody, timelines, data visualization, JavaScript, jQuery, Vis.js**

I. Introduction

Forensic investigations consist of the process of preservation, identification, extraction, documentation, and interpretation of computer data [1]. This process not only has to be completed in whole but needs to be documented meticulously for each step in the process to keep the validity of the investigation intact. Forensic investigators can do this by submitting a formal report, a preliminary written report to their own attorneys, and an examination plan to the attorneys requesting their services [2]. Another important aspect of this process includes chain of custody forms. Chain of custody forms are vital in that specific details of the evidence must be recorded from the beginning to end of an investigation. This careful documentation allows forensic investigators to further prove the integrity of their evidence in court because they were effectively in control and aware of anyone who came into the contact from when they received it to when it was presented in court.

Since cases, many times, can take months or years to actually be presented in court, there is a need to preserve this data in a way that is simple for the forensic investigator to easily review in the future. This paper proposes the development of a web based, interactive timeline data visualization tool that graphically displays the contents of a chain of custody evidence report(s).

II. Methodology: Why Visualize Data in Timelines

Timeline representation is used in many different areas and in many different professions. The idea behind timelines is the simple concept of being able to plot different steps or sequences of events in a chronological way [3]. There are three core fundamentals when it comes to timelines that are important to understand: timelines are linear, timelines are global, and timelines are literal. These three core fundamentals of timelines each pose their own problem. The linearity of a timeline does not allow it to show loops or conditions and makes the user jump around the timeline to view different events that the user might have wanted to display in a different order. The globality of the timeline makes it hard to visualize if there are a large number of objects, and the literalness of a timeline does not allow for loose expressions as all time must be exact [3].

In the proposed application, the timeline meets these requirements and thus is linear, global, and literal. To address the problem of linearity, a table was created below the timeline that acts as both a reference and as an alternative way to digest the data. To address the problem of globality, a zoom in and out function was added to the timeline. When maximally zoomed out, the function allows approximately three months of saved cases, at a time, to be viewed. When maximally zoomed in, one day of cases and the case data can be viewed; in addition, this data is separated into four hour intervals. It is also important to note that the literalness required by a timeline fits the needs of a representation of a chain of custody report as the ‘in’ and ‘out’ times are precisely recorded to hold up in court.

III. Related Work

A. Common Commercial Tools

There are many commercial tools on the market that are used extensively in computer forensics. Some examples of these are: Encase, FTK, X-Ways Forensics, MacQuisiton, and Sleuth kit/Autopsy, to name a few. Encase, was created by Guidance Software, and is known as the largest digital forensic software suite available [4]. It has the ability to identify a large quantity of different file systems and also has the ability to show file timestamps on a graphical timeline.

978-1-7281-0137-8/19/$31.00 ©2019 IEEE

FTK, also known as the Forensic ToolKit, was developed by AccessData and can also analyze many different file systems; it also specializes in carving files from free space and viewing different types of evidence types. FTK allows the viewer to view timestamps of electronic data and of the case, but does not give an overview of all the data collectively. Sleuth kit/Autopsy is a forensic suite of Unix tools put together that have a GUI. They allow the user to analyze different file systems and recover deleted files. It also shows the files chronologically but does not display them with a timeline overview [4]. These tools are mainly used during the analysis phase of an investigation. Little research is available that addresses enhancements and automation of the identification and collection phases of an investigation. However, research and tools are needed that can improve the digital forensic investigation process from the identification phase to the presentation phase of an investigation. Many of the above mentioned tools lack support in the detailed visualization of their timestamps and in a graphic visualization overview of a timeline in general.

Another observation is that proprietary/commercial tools' source code is not open to the public for modification or use. Autopsy/Sleuthkit is open source and free to download but their timeline analysis focuses on obtaining timestamp information from files and web artifacts mainly. It then has two display modes. The first can be viewed as a bar chart that shows the amount of data in a given time frame. The second gives details about the events that occurred and uses a clustering system to do so [6].

B. CyberForensic TimeLab

Upon researching tools that provided timeline and graphical visualization in digital forensics, the CyberForensic TimeLab tool was found. CyberForensic TimeLab is an open source forensic timeline prototype developed by Jens Olsson and Martin Boldt at the Blekinge Institute of Technology in Ronneby, Sweden [4]. It is divided into two main parts: the Scanner and the Viewer. The scanner is meant to scan a hard drive or other evidence recursively and to store the timestamps found. The resulting output is stored in XML format and is then viewed by the Viewer and indexed and displayed as a graphical timeline [4].

Similar to Encase and FTK, this tool supports the analysis of evidence items. However, the tool does not address the documentation and chain of custody necessities required in the identification and collection phases of an investigation. In addition, this application was published in 2009 and the code, available on GitHub, was uploaded in 2012 and has not been updated since then.

C. Mobile Applications and Models in Digital Forensic Investigations

Several methodologies and frameworks have been proposed for digital forensic investigations [4], [8] - [11]. The problem is that many methodologies focus on the analysis phase of an investigation. Although the analysis and reconstruction of the evidence are important in a digital forensic investigation, the identification and collection of evidence items are also important; in addition, models, methods, and tools that focus on this step in the investigation are greatly needed, especially tools that provide some level of automation. A mobile application tool has been proposed to assist first responders in the identification and development phases of an investigation [8]. Although proposed, an actual usable tool was not developed. Tool development and testing are critically needed in digital investigation, especially in the identification and collection phases of an investigation.

IV. TOOL DEVELOPMENT

In order to address the need for chain of custody support in the identification and collection phases of a digital forensic investigation, a web based forensic timeline data visualization forensic tool was developed. The tool takes the chain of custody input in the form of an HTML form and outputs it into two objects: the timeline and the table. The timeline visualization was visually created with help of the vis.js library.

A. Vis.js Library

Vis.js is a dynamic, browser based data visualization JavaScript library. It is designed to be easy to use, to handle large amounts of dynamic data, and to allow manipulation of and interaction with the data. The library consists of the components DataSet/DataView, Timeline, Network, Graph2d, and Graph3d [5] as shown in Figure 1.

1) Components

a) DataSet: A flexible key/value based data set. One can add, update, and remove items. A DataSet can also filter/order items.

b) DataView: A filtered or formatted view on a DataSet

c) Network: Displays a network consisting of nodes and edges. Network uses HTML canvas for creating the visualization.

d) TimeLine: An interactive visualization chart to show data in time. It can take place on a single date, or have a range (start – end date). Timeline uses HTML DOM to create the timeline.

e) Graph2d: A visualization chart creator for 2D graph creation. Graph2d uses HTML DOM and SVG for creation.

f) Graph3d: A visualization chart creator for 3D graph creation. It also supports graph animation. Graph3d uses HTML canvas for graph creation.

B. TaffyDB Library

TaffyDB, aka taffy.js, is an open source JavaScript library that provides powerful in-memory database capabilities to both browser and server applications [7].

TaffyDB was developed to create easy manipulation of object literals that are wrapped in arrays to reduce development time, improve performance, simplify maintenance, and increase quality [7].

1) Features:

a) Extremely fast

b) Powerful JavaScript-centric data selection engine

c) SQL inspired features: insert, update, unique, count, etc

d) Robust crows browser support

e) Easily extended with custom functions

f) Compatible with any DOM library (ex: jQuery, Dojo, etc.)

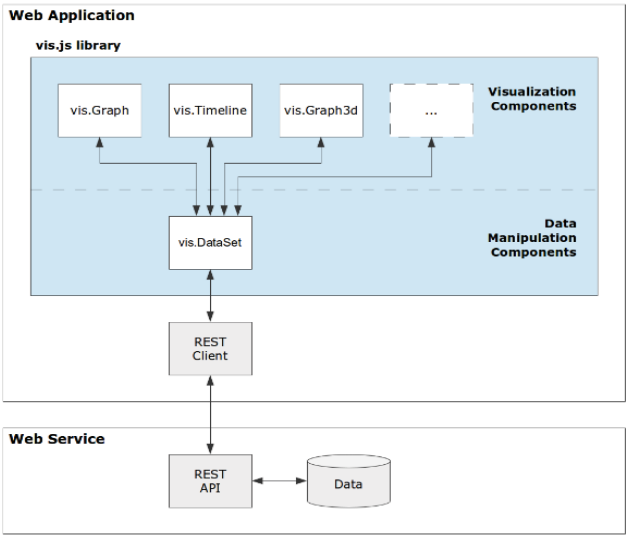


Fig. 1. Explanation of Vis.js library components [5]

C. Timely Timeline Forensic Tool: Overview

The timeline data visualization tool was developed as a web app that can be accessed locally and completely offline with the only dependencies being the Vis.js library, the TaffyDB library, and jQuery.

The web page (shown in Figure 2) has three main components: the HTML form, the table, and the timeline. The HTML form takes the input about the evidence found and has three output options. The first option is to load the data to the table which is displayed on the majority of the right side of the page. The second option is to populate the timeline which is displayed on the top of the webpage. Lastly, the third option is to save the form data in .csv file that automatically opens on click in an excel document in a preformatted table format that mirrors the table.

D. Timely Timeline Forensic Tool: System Description

The forensic tool consists of multiple custom files: index.html, script.js, timeline.js, and index.css. There are also the vis.js, TaffyDB, and jQuery dependency files.

Index.html is the only HTML file and acts as the main structure of my web app. It encompasses the form, initializes the vis (visual) timeline, holds the structure of the table, and loads all of my dependencies, scripts, and css files.

Script.js is my main JavaScript file. It is where the table is formatted. The creation of this table is done via the definition of a <table> tag and then choosing the appropriate names for the associated columns and rows. Furthermore, another task completed in this file is loading the array of input values from the HTML form into local storage and then outputting them into a JSON object that is able to be read and displayed by the vis timeline. The last two tasks completed in this script is conversion of the table input into a .csv file which is initiated on mouse clock of the 'save' button and a clear function for the table and timeline data which is linked with the reset button.

Fig. 2. View of Webpage of forensic tool Timely

The other JavaScript file, timeline.js, is where the initialization of the timeline and options are found. Technically, the timeline is initialized in index.html in the creation of the element 'visualization'. However, this vis timeline element is grabbed via the function 'document.getElementById('visualization')' in timeline.js. The component 'DataSet', while included to manipulate the data of the timeline, is initialized as empty since all of the data that we use is dynamically input into the HTML form. The options included allow for some of the interactive qualities of the table such as the min and max date allowable and the zoom functions.

E. Timely Timeline Forensic Tool: Features/Images

The chain of custody digital forensic timeline has multiple features. These features include:

- Form Features:
  - Highlighted form fields to increase readability

- Hover tooltips on field forms to increase ease of use
- Simple and straight forward buttons:
    - Load: to load data to table
    - Populate: to populate the timeline
    - Save: to download the table data in .csv Excel document
    - Reset: to clear the table and timeline data
        - Implemented with a warning prompt in case of accidental press

- Table Features:
    - Easy to read format that can be referenced via the timeline by case number
    - Holds 18 rows by default but adds a scroll function when it reaches this giving it infinite availability to hold row inputs
    - Automatic fitting of timeline based on number of items
    - Offline capability

- Timeline Features:
    - Interactive with horizontal scrolling
    - Can handle multiple items
    - Zoom feature:
        - Max zoom in: 4 hour intervals of 1 day
        - Max zoom out: 3 months at a time
    - Tooltip on hover (ex: displays investigator's name)
    - Offline capability

Not discussed previously, but one of the most important features listed above is its complete offline capability. Digital forensics investigators come into contact with information and evidence that must be protected securely. However, with the growing amount of security breaches that occur, it is getting more difficult to find security in any online forensic tool. This application combats that in its ability to be used offline and still maintains full functionality, which safeguards it from malicious attacks and only allows local usage.

Below are close up images of the tool: the HTML form (see Fig. 3), the table (see Fig. 4), the timeline (see Fig. 5), and the saved timeline.csv excel document that was created on save (see Fig. 6).

V. Future Work

Opportunities to improve the tool exist. The first improvement would be add the ability to sort/filer results in the table. Another enhanced feature would be adding the ability to search in the table and the timeline. Lastly, instead of only exporting information from the form, enhancing the tool with the ability to import pictures and files into the form would be beneficial in that all the case information collected at this point would be accessible in one place. All of these features would allow for easier access to and viewing of the data stored in the web app.

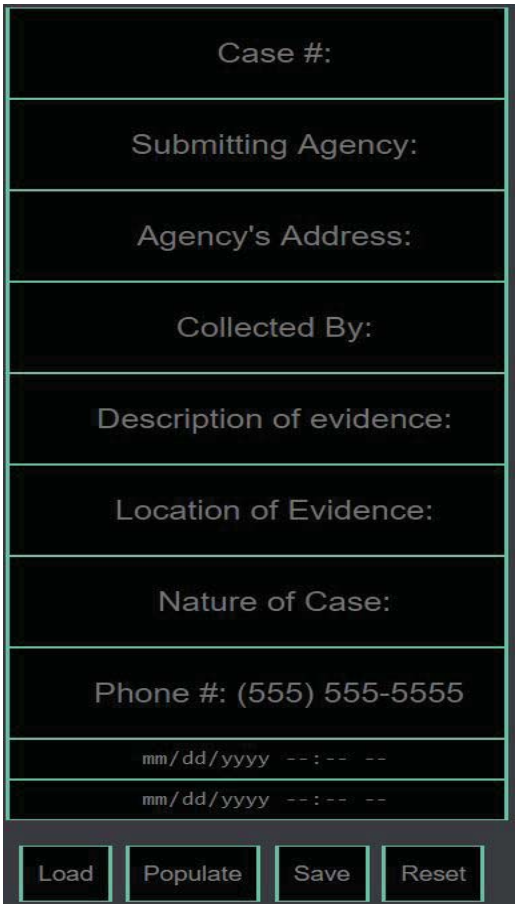


Fig. 3. HTML form for user input

History of Timeline:

Case #:	Agency Name:	Agency Address:	Collected By:	Item Description:	Location Found:	Case Nature:	Contact:	Removed:	Returned:
5	FBI	123 Made up street	Joe Roberts	None	Ridgeland, MS	Public: Criminal	555-903-021'	2017-03-15T11:11	2017-04-06T11:11
4	DHS	789 road	sally smith	none	Nashville, Tennessee	Public: Criminal	555-554-3210	2017-03-03T01:01	2017-03-21T05:02
3	JSU Police	1400 JR Lynch Street	John Smith	2 hard drives found, 1 flashdrive	Flowood, MS	Private: Civil	555-768-0123	2017-04-11T14:22	2017-04-18T14:22
2	CIA	567 your road drive	April Tanner	fingerprints found on keyboard	Clinton, MS	Public: Criminal	601-555-1234	2017-06-03T13:01	2017-06-06T14:02
1	FBI	123 Made up street	Jason Bruno	USB drive - 2GB	Jackson, MS	Public: Civil	555-555-5555	2017-03-03T02:02	2017-03-04T20:05

Fig. 4. Table with example input

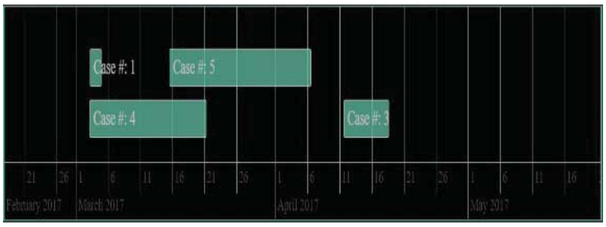
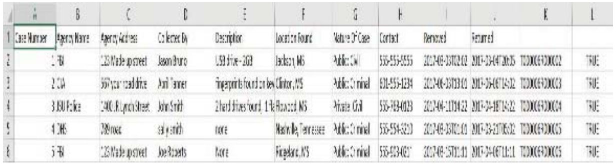


Fig. 5. Timeline with example input



	A	B	C	D	E	F	G	H	I	J	K	L
1	Case Number	Agency Name	Agency Address	Collected By	Description	Location Found	Nature Of Case	Contact	Removed	Returned		
2	1	FBI	123 Made up street	Jason Bruno	USB drive - 2GB	Jackson, MS	Public: Civil	555-555-5555	[illegible]	[illegible]	[illegible]	TRUE
3	2	CIA	567 your road drive	April Tanner	Fingerprints found on key	Clinton, MS	Public: Criminal	601-555-1234	[illegible]	[illegible]	[illegible]	TRUE
4	3	JSU Police	1400 J.R Lynch Street	John Smith	2 hard drives found, 1 fla	Flowood, MS	Private: Civil	[illegible]	[illegible]	[illegible]	[illegible]	TRUE
5	4	DHS	789 road	sally smith	none	Nashville, Tennessee	Public: Criminal	[illegible]	[illegible]	[illegible]	[illegible]	TRUE
6	5	FBI	123 Made up street	Joe Roberts	None	Ridgeland, MS	Public: Criminal	[illegible]	[illegible]	[illegible]	[illegible]	TRUE

Fig. 6. Timeline.csv file with example input

VI. Conclusions

Digital Forensics is a field that is constantly adapting to the development of new technologies and is still in high demand; however, there is a shortage of qualified investigators. Because of this, it is common for one digital forensic investigator to have multiple cases, and often times, these cases have court dates that can be months or years after the initial investigation.

Currently, reporting is demonstrated in the field with a heavy focus on handwritten reporting. The entire process must be heavily documented and detailed to hold up in court. While, compiling notes and creating a report is not extremely complex, often times these reports are quite lengthy and complex. As a result, there is a need for a digital forensic tool that allows investigators to quickly load their reports while providing a visual representation of the process.

A chain of custody timeline data visualization tool is a logical solution for this problem. It allows users to adhere to the strict guidelines that a chain of custody form requires due to the literal expectation of time inputs that the timeline assumes. It also allows compilation of case data information in one place with table reference and ability to save to .csv file for safe keeping. Given the local storage factor of the timeline data, the inputs will persist unless deleted by the user even upon exit of the application or exiting of the page. In the future, a tool that provides digital forensic case support throughout the entire process will greatly enhance digital investigations and improve the process in the age of big data.

Acknowledgments

This research was sponsored by the Defense Intelligence Agency IC CAE Grant Award #300223341A, and the U.S. Army Engineer Research and Development Center (ERDC) Strategic Cyber Science, Warfare, Security, Application Development & HPC R&D Cyber Warfare Grant #634B95.

References

[1] W. Kruse and J. Heiser,Computer Forensics: Incident Response Essentials, Addison-Wesley, Boston, Massachusetts, 2001.

[2] B. Nelsn, A. Philips, C. Steuart, Guide to Computer Forensics and Investigations, Fourth Edition, Course Technology, Boston, Massachusetts, 2010.

[3] K. Kurihara, D. Vronay, and T. Igarashi, “Flexible Timeline User Interface using Constraints”, CHI EA ’05 Extended Abstracts on Human Factors in Computing Systems, Portland OR, April 022005, IEEE, pp. 1581-1584.

[4] J. Olsson and M. Boldt, “Computer Forensic Timeline Visualization Tool”, Proceedings of The Digital Forensic Research Conference DFRWS, Montreal, Canada, August 17-19 2009, pp. 1 -11

[5] Vis.Js, [Online]. Available: https://visjs.org

[6] Sletuhkit, [Online]. Available: https://www.sleuthkit.org

[7] TaffyDB, [Online]. Available: http://taffydb.com

[8] A. Tanner and D. Dampier, “An approach for managing knowledge in digital forensic investigations,” International Journal of Computer Science and Security, vol. 4, no. 5, pp. 451-465, December 2010.

[9] A. Tanner and S. Duncan, "On Integrating Mobile Applications into the Digital Forensic Investigative Process," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 8, September 2013, pp. 56-61.

[10] M. Reith, C. Carr, and G. Gunsch, “An Examination of Digital Forensic Models,” *International Journal of Digital Evidence*, vol. 1, no. 3, Fall 2002, pp. 1—20.

[11] M. Pollitt, “An Ad Hoc Review of Digital Forensic Models,” *Proceedings: Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, Bell Harbor, Washington, Apr. 2007, IEEE, pp. 43—54.