Emoji-nized Log Browser: Visualization of Server-logs by Emoji for System Administrators[*]

Tetsuji Takada
The University of Electro-Communications
Chofu, Tokyo, Japan
zetaka@computer.org

Takaaki Abe[†]
The University of Electro-Communications
Chofu, Tokyo, Japan
tkakab050203@gmail.com

ABSTRACT

We propose a log data visualization system by Emoji (pictorial symbol). A log inspection and its monitoring are essential task for system administrators to be aware of anomalous status of the IT systems and security incidents. Information visualization is a promising approach to assist the task. However, there is no visualization work to support understanding the textual data more directly. We, then, propose a text visualization by replacing text data with emoji based on a user-defined rule. In this paper, we explain an idea of visualization by emoji, and we also introduce a prototype system based on the idea for an access log of a web server. We also discuss about expected advantages and future work.

CCS CONCEPTS

• **Human-centered computing** → **Visualization systems and tools**; Ubiquitous and mobile computing systems and tools; • **Security and privacy** → *Usability in security and privacy*; • **Information systems** → Web applications;

KEYWORDS

Emoji, Pictgraph, Information visualization, Log data, System administrator

1 INTRODUCTION

Log data is an important information source especially for system administrators (*sysadmins*). Monitoring and inspecting the log data is an essential task for them to be aware of anomalous status of IT systems and security incidents. However, log data is generally a large amount of textual information. Therefore, it is hard for sysadmins to perform the task because they have to read, understand and extract necessary or useful information from the data. This is not only tedious and time-consuming task but also a knowledgeable task. A support system is desired for performing the task.

Information visualization is one of the schemes for this purpose [4–8]. This scheme generally provides a global view of the data for assist understanding an overview of the data or a designed view for finding a specific data that sysadmins should pay attention to. However, even if such views are provided, there is still needed to look at textual log data. The reason is that sysadmins need to know the detail of what happened when they found useful data from the global or designed views.

In this paper, we report on a trial of visualization of textual log data by Emoji (Pictographs). Emoji is a pictorial symbol [3], but it is also available as a character. By replacing a part of log messages with emoji(s), the log inspection task changes from “reading and understanding text data” to “viewing pictographic symbols”. We expect that this change contributes to reduce the task load in a log inspection.

2 EMOJI-NIZED LOG BROWSER

Log data consists of many log messages, and each log message is generally composed more than one data element (e.g. datetime, IP address, URL, etc). Each value of the elements is usually a discrete value or a value in a defined range. We replace the data elements with emoji based on a user-defined rule as a textual data visualization.

We did not make a completely different view with 2D or 3D graphics, because our aim is to directly assist log inspection task by sysadmins. Since emoji has a feature of both a visual symbol and a character, visualization of textual data can be done by a simple substitution.

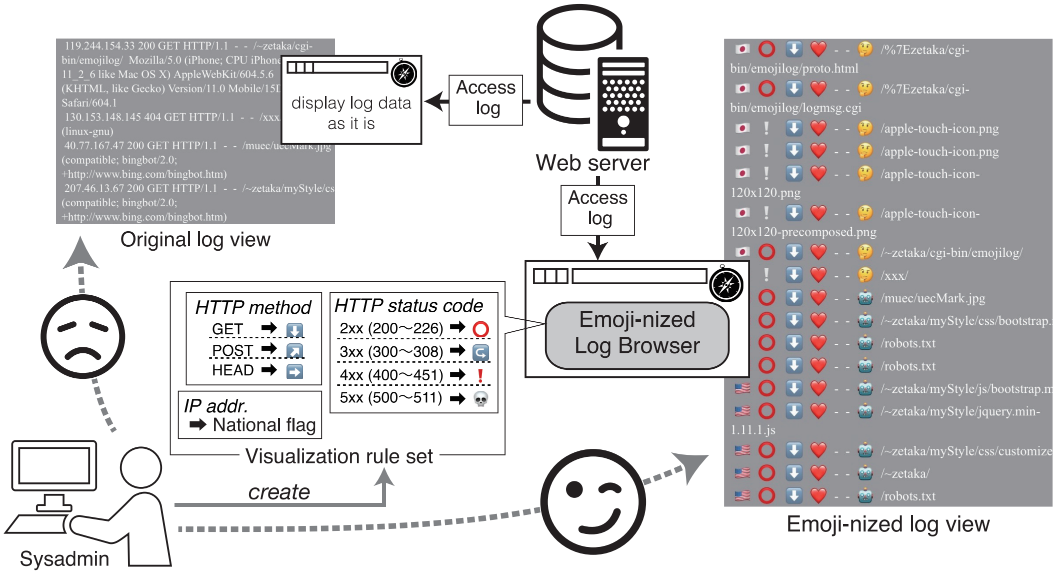
We have implemented a prototype visual log browser, named “Emoji-nized Log Browser” (*ELB*). This system focuses on visualizing an access log of “Apache Web server” [1], and it is also implemented as a web application so that it can be used even from mobile terminals. We explain how to use the *ELB*.

At first, a user has to define a visualization rule set. Each rule has both a target string/value and a substitution symbol(emoji). And a user sets the defined rule set to *ELB*. When the *ELB* starts running, *ELB* obtains original log data from a web server, and replaces targeted data elements in log messages with emoji based on the applied rule set. A user, then, can browse visualized log data (a screen snapshot in the right side of the Fig. 1).

We explain some of rules that were defined for visualizing a web server access log as follows.
a) **Word based rule**: We replace a specific word with one or some emoji(s). We use this rule for visualizing “HTTP method” (Fig. 1).
b) **Range of Values based rule**: We replace values in a certain range with one or some emoji(s). We use this rule for “HTTP status code”. A response code 2xx (a value range is actually 200-206) is substituted with a circle emoji because these values represent successful operations.

[*] This paper is revised a bit from the original version in ACM Digital Library.
[†] He already graduated and is woking on a private company.

AVI'18, May 29-June 1, 2018, Castiglione della Pescaia, Italy
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5616-9/18/05.
https://doi.org/10.1145/3206505.3206578



```
 119.244.154.33 200 GET HTTP/1.1  -  -  /~zetaka/cgi-
bin/emojilog/  Mozilla/5.0 (iPhone; CPU iPhone
11_2_6 like Mac OS X) AppleWebKit/604.5.6
(KHTML, like Gecko) Version/11.0 Mobile/15D
Safari/604.1
 130.153.148.145 404 GET HTTP/1.1  -  -  /xxx
(linux-gnu)
 40.77.167.47 200 GET HTTP/1.1  -  -  /muec/uecMark.jpg
(compatible; bingbot/2.0;
+http://www.bing.com/bingbot.htm)
 207.46.13.67 200 GET HTTP/1.1  -  -  /~zetaka/myStyle/cs
(compatible; bingbot/2.0;
+http://www.bing.com/bingbot.htm)
```

```
🇯🇵 ⭕ ⬇️ ❤️ - - 🤔 /%7Ezetaka/cgi-
bin/emojilog/proto.html
🇯🇵 ⭕ ⬇️ ❤️ - - 🤔 /%7Ezetaka/cgi-
bin/emojilog/logmsg.cgi
🇯🇵 ❕ ⬇️ ❤️ - - 🤔 /apple-touch-icon.png
🇯🇵 ❕ ⬇️ ❤️ - - 🤔 /apple-touch-icon.png
🇯🇵 ❕ ⬇️ ❤️ - - 🤔 /apple-touch-icon-
120x120.png
🇯🇵 ❕ ⬇️ ❤️ - - 🤔 /apple-touch-icon-
120x120-precomposed.png
🇯🇵 ⭕ ⬇️ ❤️ - - 🤔 /~zetaka/cgi-bin/emojilog/
   ❕ ⬇️ ❤️ - - 🤔 /xxx/
   ⭕ ⬇️ ❤️ - - 🤖 /muec/uecMark.jpg
   ⭕ ⬇️ ❤️ - - 🤖 /~zetaka/myStyle/css/bootstrap.
   ⭕ ⬇️ ❤️ - - 🤖 /robots.txt
   ⭕ ⬇️ ❤️ - - 🤖 /robots.txt
🇺🇸 ⭕ ⬇️ ❤️ - - 🤖 /~zetaka/myStyle/js/bootstrap.m
🇺🇸 ⭕ ⬇️ ❤️ - - 🤖 /~zetaka/myStyle/jquery.min-
1.11.1.js
🇺🇸 ⭕ ⬇️ ❤️ - - 🤖 /~zetaka/myStyle/css/customize
🇺🇸 ⭕ ⬇️ ❤️ - - 🤖 /~zetaka/
🇺🇸 ⭕ ⬇️ ❤️ - - 🤖 /robots.txt
```

Figure 1: An Process Overview and a Snapshot of Visualized log view of Emoji-nized Log Browser

c) **Rule with an extra interpretation**: We use this rule for visualizing IP address. We retrieve a country code from each IP address using a geo-location service [2], and the code is visualized by an emoji of a national flag.

We consider that *ELB* can provide the following advantages to sysadmins.

(1) **Task load reduction**: Since a part of each log message is visualized, an actual task changes from "reading text messages and understanding the meaning of them" to just "looking visual symbols in log messages". This could reduce the task load in a log inspection. Moreover, as a side effect of this visualization, the amount of characters presented to sysadmins is reduced. We consider that ELB could summarize the log data by a visualization. This feature could also contribute a task load reduction.

(2) **Embedding a meaning and an interpretation of the data into visualization**: A user can reflect a meaning and/or an interpretation of each data element in log messages to visualization rule. If a data element in a log message represents successful operation, the element is replaced with a circle emoji in order to indicate successful operation, and if not, it is substituted with an emoji of a red cross or a warning sign. This means that our scheme has flexibility that enables not only to visualize log data but also to give a visual representation of its meaning and interpretation. This is useful for (1) finding a meaningful data, (2) not to misinterpret data, and (3) not to overlook a meaningful data.

(3) **Personalization and Reuse various knowledges**: *ELB* allows sysadmins to customize a visual design of log data according to their needs, and the way is just creating their own visualization rule set. In other words, ELB enables users to use a personalized visual representation. Moreover, we will implement a web system for sharing user-defined visualization rule sets with others, This enables sysadmins to reuse a wide variety of visualization rule sets created by others. tips for a log inspection. This could assist log inspection task using other engineer's knowledge or tips for a log inspection task. It would also be useful for training a log inspection task for a novice sysadmin.

3 CONCLUSIONS AND FUTURE WORK

We presented "Emoji-nized log browser" (*ELB*) that visualizes log data by emoji based on a user-defined rule. We consider that this is a unique approach in information visualization because our scheme makes use of an emoji as a visualization unit instead of generating a completely different view by a graphical representation. The *ELB* has a potential to reduce the task load in a log inspection. The visualization with emoji simplifies the task of "reading and understanding textual information" to the task of "looking at emoji-nized messages". Moreover, *ELB* could embed "meaning and interpretation of data" in the visual representation. This feature makes it possible for a novice system administrator to perform a log inspection with expert sysadmin's knowledge.

Although we have got positive opinions to the *ELB* from informal interviews with a few sysadmins, we have not evaluated *ELB* yet. We have to conduct an evaluation experiment on a task load mitigation with system administrators. We also have system enhancement plans as follows: (1) Designing an another view to provide both an overview and a different insight of log data, (2) Developing data summarization scheme that can summarize multiple lines of log messages into a fewer messages: Data summarization of *ELB* is performed for each log message. With this scheme, it is impossible to reduce the number of log messages that sysadmins have to look. We consider another data summarization scheme to be able to reduce the number of log messages. (3) Interactive functions for data filtering and detail data retrieval, and (4) Support systems that enables to assist a visualization rule creation and its sharing with others. Finally, although we consider that there is no critical issue, we also examine the applicability of other kind of log data.

REFERENCES

[1] The Apache Software Foundation. [n. d.]. Apache HTTP Server Project. ([n. d.]). Retrieved March 12, 2018 from https://httpd.apache.org/

[2] MaxMind Inc. [n. d.]. Open Source Data and APIs - GeoLite2 Data. ([n. d.]). Retrieved March 12, 2018 from https://www.maxmind.com/en/open-source-data-and-api-for-ip-geolocation

[3] Unicode Inc. [n. d.]. Full Emoji List, v11.0. ([n. d.]). Retrieved March 12, 2018 from https://unicode.org/emoji/charts/full-emoji-list.html

[4] H. Shiravi, A. Shiravi, and A. A. Ghorbani. 2012. A Survey of Visualization Systems for Network Security. *IEEE Transactions on Visualization and Computer Graphics* 18, 8 (Aug 2012), 1313–1329.

[5] J.-E. Stange, M. Dörk, J. Landstorfer, and R. Wettach. 2014. Visual Filter: Graphical Exploration of Network Security Log Files. In *Proc. of the Eleventh Workshop on Visualization for Cyber Security (VizSec '14)*. 41–48.

[6] T. Takada and H. Koike. 2002. MieLog: A Highly Interactive Visual Log Browser Using Information Visualization and Statistical Analysis. In *Proc. of the 16th USENIX Conference on System Administration (LISA '02)*. 133–144.

[7] T. Takada and H. Koike. 2002. Tudumi: information visualization system for monitoring and auditing computer logs. In *Proc. Sixth International Conference on Information Visualisation*. 570–576.

[8] R. Vuillemot, J. Boy, A. Tabard, C. Perin, and J.D. Fekete. 2016. Challenges in Logging Interactive Visualizations and Visualizing Interaction Logs. In *Proc. of Workshop on Logging Interactive Visualizations and Visualizing Interaction Logs*.