JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

FORENSIC ANALYSIS OF DIGITAL ARTIFACTS OF QR CODE PHISHING ATTACK AT 'AISYIYAH UNIVERSITY YOGYAKARTA

Arizona Firdonsyah[1], Yunan Al-Husaini Djaibakal[1*]
[1]nformation Technology' Aisyiyah University Yogyakarta
email: *yunandjaibakal@gmail.com

Abstract: The use of QR Codes in academic settings has increased with the digitization of attendance systems, but it has also introduced potential abuse in the form of quishing attacks (QR phishing). Previous studies have mainly focused on user behavior, while forensic analysis of digital artifacts as evidence is still limited. This study aims to conduct a forensic analysis of browser artifacts resulting from interactions with dangerous QR Codes at Aisyiyah University Yogyakarta using the framework of the National Justice Institute (NIJ). Six investigation parameters are defined: domain identification, endpoint identification, identification of supporting resources, visualization of image artifacts, timestamp correlation, and HTML reconstruction. Data is obtained from the Google Chrome profile directory and analyzed using Autopsy, focusing on Web Cache, Browser History, and Cookies artifacts. The results showed that five parameters were successfully identified with an investigation success rate of 83.3%, while HTML reconstruction could not be fully achieved due to cache limitations. These findings show that Web Cache artifacts provide evidentiary value in the forensic investigation of QR Code-based attacks. Future research should focus on improving full-page reconstruction techniques.

Keywords: browser forensics; digital artifacts; NIJ; quishing; Web Cache

Abstrak: Penggunaan Kode QR di lingkungan akademik telah meningkat seiring dengan digitalisasi sistem absensi, tetapi juga menimbulkan potensi penyalahgunaan dalam bentuk serangan phishing (QR phishing). Studi sebelumnya sebagian besar berfokus pada perilaku pengguna, sementara analisis forensik artefak digital sebagai bukti masih terbatas. Studi ini bertujuan untuk melakukan analisis forensik artefak browser yang dihasilkan dari interaksi dengan Kode QR berbahaya di Universitas 'Aisyiyah Yogyakarta menggunakan kerangka kerja Lembaga Kehakiman Nasional (NIJ). Enam parameter investigasi didefinisikan: identifikasi domain, identifikasi titik akhir, identifikasi sumber daya pendukung, visualisasi artefak gambar, korelasi stempel waktu, dan rekonstruksi HTML. Data diperoleh dari direktori profil Google Chrome dan dianalisis menggunakan Autopsy, dengan fokus pada artefak Cache Web, Riwayat Browser, dan Cookie. Hasil menunjukkan bahwa lima parameter berhasil diidentifikasi dengan tingkat keberhasilan investigasi sebesar 83,3%, sementara rekonstruksi HTML tidak dapat sepenuhnya dicapai karena keterbatasan cache. Temuan ini menunjukkan bahwa artefak Cache Web memberikan nilai bukti dalam investigasi forensik serangan berbasis Kode QR. Penelitian selanjutnya harus fokus pada peningkatan teknik rekonstruksi halaman penuh.

Kata kunci: forensik peramban; artefak digital; NIJ; quishing; web cache

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

The development of digital technology encourages the use of QR Codes in various information-based service systems, including in the academic environment. The application of QR Codes in the attendance system has been proven to increase the efficiency and accuracy of attendance recording [1]. At Aisyiyah University Yogyakarta, QR Codes are used as a mechanism for lecture attendance, so that scanning activities become part of the student's academic process.

The technical characteristics of QR Codes allow abuse in the form of quishing attacks (QR phishing), where users can be redirected to malicious pages without realizing it [2][3]. Previous research has shown that users are more likely to access scanned links without advanced verification [4][5]. and the ease of creating QR Codes increases the potential for malicious link insertion [6][7].

Previous research has extensively addressed the threat of quishing in public spaces and public environments [8][9], as well as emphasizing aspects of security and user behavior [10][11]. However, the analysis of digital artifacts after interaction with malicious QR Codes is still limited, especially in the context of an academic environment. This shows that there is a research gap in the use of digital artifacts as the basis for forensic evidence.

D In this study, it was found that an unofficial QR Code was used as a media presence within Aisyiyah University of Yogyakarta. The search results show that the QR Code is not registered as the official campus system, thus indicating potential misuse and becoming the basis for a forensic investigation into the Google Chrome browser artifact.

Browser artifacts such as browser history, Web Cache, and cookies can be used to reconstruct access activity based on domain, endpoint, and timestamp correlations [12][13]. Web Cache stores the responses of pages and resources loaded by the browser, thus allowing the identification of content that has been accessed. Based on this, this study aims to analyze browser digital artifacts to identify access traces and reconstruct the chronology of activities. This research contributes by showing that Web Cache artifacts can be used as forensic evidence as well as proposing browser artifact-based investigative parameters in the case of quishing.

METHODS

This study uses the National Institute of Justice (NIJ) framework which consists of the stages of Preparation, Collection, Examination, Analysis, and Reporting [14][15]. This method is used to analyze digital artifacts in the Google Chrome browser generated after phishing QR Code access in the Aisyiyah University of Yogyakarta environment.

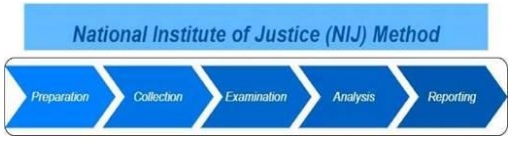

Figure 1. NIJ Method

Preparation

In the preparation stage, the analyzed artifacts are determined, namely browser history, Web Cache,

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

and cookies, as well as six investigation parameters: domain identification, endpoints, supporting resources, image artifact visualization, timestamp correlation, and HTML reconstruction [13].

Collections

The collection stage is carried out by duplicating the Google Chrome profile directory to generate a working copy, then verifying using a hash to maintain data integrity.

Examination

The examination stage is performed using Autopsy with a focus on Web Cache to identify domains, endpoints, resources, and access timestamps.

Analysis

The analysis stage is done through domain, endpoint, and timestamp correlation to compile the sequence of access activities and identify the resources that are loaded. The chronological reconstruction is the result of the analysis and does not include the investigation parameters.

Reporting

This stage documents the results of the investigation in the form of screenshots of artifacts, tables of findings, and chronological reconstruction of access. This report is compiled based on the identified digital artifacts without adding assumptions outside of the data.

RESULTS AND DISCUSSION

This section presents the results of the Google Chrome browser artifact analysis based on NIJ stages for phishing QR Code access.

Preparation

The preparation establishes the scope of the investigation by determining the analyzed artifacts, namely Browser History, Web Cache, and Cookies in the Google Chrome profile directory, as well as the use of Autopsy as an analysis tool and Windows PowerShell for verification of integrity through hash values. Separation between the original data and the working copy is done to maintain the integrity of the artifacts during the analysis process, with the configuration of this stage summarized in Table 1.

Table 1. Stage Configuration Preparation.

Components	Remarks
Digital Artifacts	Browser History, Web Cache, Cookies
Target Apps	Google Chrome (Default Profile)
Artifact Source Location	Chrome Profile Directory on Windows
Tool Analysis	Autopsy
Integrity Verification Tool	Windows PowerShell (Get-FileHash SHA-256)
Objectives of the Preparatory Stage	Establish scope and maintain the integrity of artifacts prior to acquisition

Collections

The collection stage is done by duplicating the Google Chrome profile directory to generate a working copy, while the original data is retained. The integrity of the data is verified using the SHA-256 algorithm, where the similarity of the hash value between the original and duplicate data indicates no change during the acquisition process Table 2.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Examination

The examination stage was carried out using Autopsy with a focus on analyzing Web Cache artifacts to identify domains, endpoints, resources, and timestamps related to phishing QR Code access activities. The results of the analysis show the presence of the target domain along with *the /Login/dashboard* endpoint with the access time recorded in the system, which is further presented in Figure 2 and Table 3.

Analysis Domain and Endpoint Identification

The results of the analysis show that the browser accesses the primary domain and navigates to the */Login/dashboard* endpoint in a single consistent session based on timestamp correlation Table 4.

HTML Reconstructing Efforts

The cache file (data_1) is stored in application/octet-stream format, making the HTML structure unreadable. This shows that HTML is not stored in full text form, with the results of the analysis presented in Figure 3 and Table 2.

Table 2. Analyze cache endpoint files.

Parameters	Results
Cache File Name	data_1
Artifact Location	Cache/Cache_Data
Related Endpoints	/Login/dashboard
MIME Types	Applications/ octet Flow
File Size	794.624 bytes
Storage Format	Compressed binary data
Readable HTML Structure	No
Reconstruction of the Whole Scene	Not doable

Visual Evidence of Cache Artifacts

The cached artifact successfully displays the institution's logo image file through the *View Cached File feature*, which indicates that the page has been loaded by the browser.

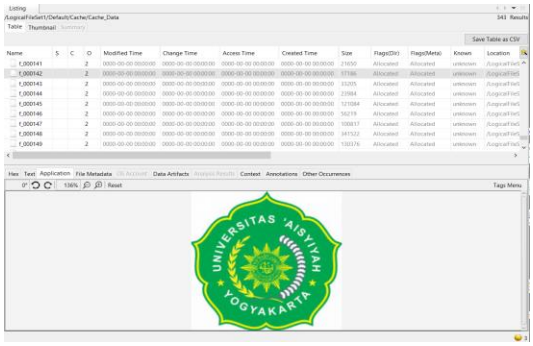

Figure 2. Visualization of logos from cache

Access Chronological Reconstruction

The correlation of domains, resources, and timestamps shows the sequence of activities in a single consistent access session, as summarized in Table 6.

Limitations of Reconstruction

The cache files associated with the endpoint are stored in the application/octet-stream, so that the HTML structure cannot be reconstructed in its entirety, the technical characteristics of the cached file are summarized in Table 3. This is in line with modern browser caching mechanisms that do not always maintain HTML structures in the form of open text [13].

Table 3. Technical Parameters File cache.

Parameters	Results
File Name	data_1
Artifact Location	Cache/Cache_Data
Related Endpoints	/Login/dashboard
MIME Types	Applications/Octete *stream*

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Reporting

The Reporting Stage presents the final results of the investigation based on *the* National Institute of Justice (NIJ) method. Web Cache artifact analysis successfully identifies domains, endpoints, supporting resources, and access activity based on timestamps, and image visualization shows that the page has been loaded by the browser. However, HTML structure reconstruction cannot be done in its entirety due to the limitations of the caching mechanism. A summary of the process and findings of the investigation are presented in Table 4.

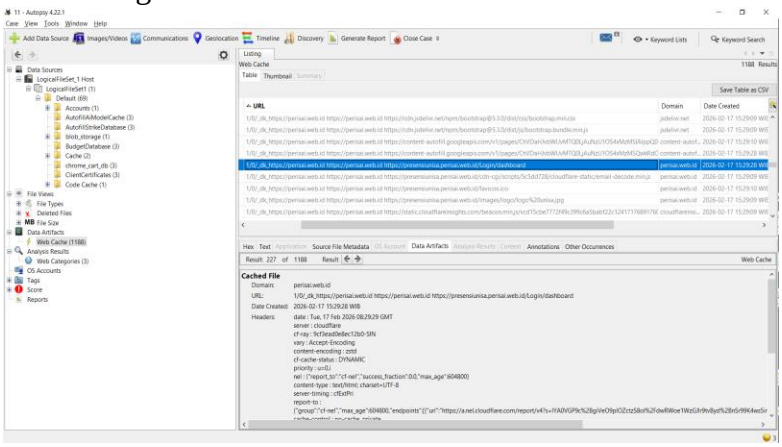

Figure 4. Identify Web Cache artifacts.

Figure 5. File Cache (data_1)

Table 2. Verify the integrity of artifacts

Data Components	Algorithm	Hash Value (SHA-256)	Remarks
Original Data	SHA-256	F2B8C2293BDDA6E338A44B6F733B 9B351BE9B2F2A7F2D2C4E9A86BACC3DA	Identical
Duplicate Data	SHA-256	F2B8C2293BDDA6E338A44B6F733B 9B351BE9B2F2A7F2D2C4E9A86BACC3DA	Identical

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Table 6. Web Cache Identification.

Artifact Types	Domain	Endpoints/Resources	Timestamps
Home	presensiunisa.perisai.web.id	/	15:29:09
Endpoints	presensiunisa.perisai.web.id	/Login/dashboard	15:29:28
CSS	cdn.jsdelivr.net	bootstrap.min.css	15:29:09
Script	cdn.jsdelivr.net	bootstrap.bundle.min.js	15:29:09
Image	presensiunisa.perisai.web.id	logo_unisa.jpg	15:29:09

Table 7. Domain and endpoint correlation.

Domain	Full URL	Endpoints	Timestamp (WIB)	Activity Indications
presensiunisa.perisai.web.id	https://presensiunisa.perisai.web.id/	/	15:29:09	Access the main page
presensiunisa.perisai.web.id	https://presensiunisa.perisai.web.id/Login/dashboard	/Login/dashboard	15:29:28	Advanced navigation system
cdn.jsdelivr.net	https://cdn.jsdelivr.net/.../bootstrap.min.css	CSS Resources	15:29:09	Call a support resource
cdn.jsdelivr.net	https://cdn.jsdelivr.net/.../bootstrap.bundle.min.js	Resource Scripts	15:29:09	System script loaded

Table 8. Access Chronological Reconstruction Based on cached web artifacts

Digital Artifacts	Activity Indications	Timestamp (WIB)
Access the primary domain	Browser accesses the scan results page QR code	15:29:09
CSS & JavaScript Files	Page support resources loaded by Browser	15:29:09
Institutional logo image file	Visual elements of the page are stored in Cache	15:29:09
Endpoint `/Login/dashboard`	Advanced navigation to system pages	15:29:28

Table 9. Process summary and Investigative Findings

NIJ Rate	Process	Artifacts Analyzed	Findings
Preparation	Determination of artifacts & tools	History, Cache, Cookies	The scope of the investigation is established
Collections	Duplicate & hash verification	Chrome director profile	Data integrity is maintained
Inspection	Cache artifact identification	Web Cache	Domain, endpoint, timestamp found
Analysis	Artifact correlation	Domains, resources, timestamps	Timeline access was successfully created
Analysis (Visual)	Cache visualization	Image files	Pages are proven to load
Analysis (HTML)	Cache file extraction	data_1	HTML cannot be reconstructed

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XII No 2, Maret 2026, hlm. 343 – 350 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/ 10.33330/jurteksi.v12i2.4504
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

CONCLUSION

This research shows that Web Cache artifacts in the Google Chrome browser can be used as a basis for evidence in the forensic investigation of QR Code-based quishing attacks. Using *the National Institute of Justice* (NIJ) method, a reconstruction of access activity is constructed through the correlation of domains, endpoints, resources, and timestamps. Of the six investigation parameters, five were successfully verified domain identification, endpoints, supporting resources, image artifact visualization, and timestamp correlation with an 83.3% success rate, while HTML reconstruction was unsuccessful due to caching mechanisms. These results confirm that the browser artifacts are sufficient for proof. Further research is directed at the development of HTML reconstruction and cross-device and browser analysis.

BIBLIOGRAPHY

[1] J. Hendrawan, I. D. Perwitasari, and F. Maulana, "QR Code-Based Attendance Systems in Education: A Systematic Literature Review on Data Accuracy and Sustainable School Management," *CESSMUDS 1*, no. 2020, pp. 80–87, 2024.

[2] X. Zhang *et al.*, "Demystifying (In) QR Code-based Login Security in Real-World Applications Demystifying QR Code-Based Login Security in Real-World Applications," *The 34th USENIX Security. Symptoms.*, 2025.

[3] F. Sharevski, G. Schiefer, and M. Volkamer, "Exploring Phishing Threats via QR Codes in Naturalistic Settings," *USEC 2024 SymptomsNo. February, 2024*.

[4] G. A. Amoah, "QR Code Security: Reducing Quishing (QR Code Phishing) Problems," *Int. J. Computing. Application.*Nope. October, 2022, doi: 10.5120/ijca2022922425.

[5] A. W. Tenri, F. Singkeruang, S. Ega, and S. Nuraeni, "Mitigating the Risk of Qushing Threats (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economy security," *Parade. J. Economics.*, vol. 8, no. 2, pp. 685–696, 2025.

[6] M. Kowalewski, L. Lassak, M. Dürmuth, T. Schnitzler, and the U.S. Symposium, "Scanned and Deceived: Insecurity by ObsQRity? Measuring User Vulnerability and QR Code-Based Attack Awareness," *The 34th USENIX Security. Symptoms.*, 2025.

[7] N. Nigam and R. Bhandari, "Performance Analysis of QR Phishing Detection Approach," *J. Info. Syst. Eng. Manag.*, vol. 10, pp. 221–225, 2025.

[8] M. Geisler, D. Pöhn, and W. Hommel, "arXiv : 2407 . 16230v1 [cs . CR] 23 Jul 2024 Hooked: A Real-World Study on QR Code Phishing," *arXiv: 2204.03714*, 2024.

[9] M. W. Akram, K. Sood, S. Member, and M. U. Hassan, "QR¨ ıS: A Novel Preemptive Method to Overcome Detection Through QR Structural Features," *arXiv: 2510.17175*, pp. 1–13,

2025.

[10] F. Sharevski, A. Devine, and E. Pieroni, *Gone Quishing : Phishing Field Study with Malicious QR Codes*, vol. 1, no. 1. Association for Computing Engines, 2022.

[11] J. Management and P. Finance, "QR-PHISHING RISK MITIGATION IN INDONESIAN DIGITAL PAYMENTS THROUGH THE SECURITY BEHAVIOR INTENT SCALE (SEBIS)," *J. Manaj. Perbank. Nitro*, vol. 1, no. 3, pp. 78–92, 2025, doi: 10.56858/jmpkn.v1i3.757.

[12] A. Trivedi, K. Jangal, and R. Gupta, "Phishing Detection in Advanced QR Code Attacks: AI-Based Challenges and Solutions," *IJRASETTidak. January, 2025*.

[13] D. Forensics, "Forensic Google chrome Hitesh Sanghvi Digvijaysinh Rathod*Salem Yahya Altaleedi, Abdulaziz Saleh AlThani, Mohammed Abd Alrhman Alkhawaldeh and Abdulrazaq Almorjan Ramya Shah Tanveer Zia," *Int. J. Elec. Secur. Digit. Forensic*, vol. 15, no. 6, 2023.

[14] A. Firdonsyah, "Comparative Analysis of Forensic Software for Android-based Blackberry Messenger Using NIJ Framework and NIST Measurement," *IJCSDF*, vol. 10, no. 2, pp. 78–90, 2021.

[15] A. Firdonsyah and D. Wijayanto, "Forensic Analysis of Digital Document Engineering with NIJ," *IJCSDF*, vol. 11, no. 2, pp. 34–39, 2022.