ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

LEVERAGING DIGITAL DATABASES FOR SUSPECT IDENTIFICATION:AN EVALUATION OF PHILIPPINE NATIONAL POLICE INVESTIGATIVE PRACTICES

Kathrine Joy Ong Jose
Student, Doctor of Philosophy in Criminology, Philippine College of Criminology

Article DOI: https://doi.org/10.36713/epra31324
DOI No: 10.36713/epra31324

ABSTRACT

The increasing reliance on digital technologies in law enforcement has transformed suspect identification and criminal investigation. This study evaluated the utilization and perceived effectiveness of four Philippine National Police (PNP) digital databases – the Automated Fingerprint Identification System (AFIS), e-Rogues Gallery, Crime Information, Reporting and Analysis System (CIRAS), and e-Warrant System – among investigators and intelligence operatives in the National Capital Region Police Office (NCRPO). It further examined the relationship between perceived database effectiveness and investigative outcomes in terms of speed, accuracy, and case resolution, explored the lived experiences of PNP personnel, and developed an intervention framework based on the findings. An explanatory sequential mixed-methods design was employed. Quantitative data were obtained from 509 respondents using a researcher-made questionnaire, while qualitative data were gathered through structured interviews with 10 key informants. Median and interquartile range were used for descriptive analysis, while Spearman rank-order correlation was used to examine relationships among ordinal variables. The qualitative data were analyzed through thematic analysis. The findings showed uniformly high utilization of the four databases, with respondents generally rating the systems as always utilized and highly effective across speed, accuracy, and case resolution. Spearman correlations were positive and highly significant across all database-outcome pairs ($p < .001$). Qualitative findings, however, identified operational vulnerabilities involving internet dependence, system interruptions, restricted access, training and technical competence, and incomplete, outdated, or inaccurate records. The study proposes the Digital Investigative Capability and Resilience Framework (DICRF), which emphasizes offline continuity, multi-tiered role-based access, proactive record updating, specialized digital competency, and secure cross-jurisdictional information sharing. The study concludes that digital databases have become essential to modern PNP investigations, but sustained investigative effectiveness requires resilient infrastructure, accurate data, appropriate access controls, and continuing technical capacity development.

KEYWORDS: *Digital Databases; Suspect Identification; AFIS; E-Rogues Gallery; CIRAS; E-Warrant System; Investigative Effectiveness; Philippine National Police; NCRPO*

1. INTRODUCTION

Background and Research Problem

Personal identification is a fundamental component of criminal investigation because law enforcement must determine the identity of individuals connected with criminal activity. Traditional identification depended heavily on witness accounts, physical descriptions, handwritten records, and paper-based fingerprint comparison. These processes could be time-consuming, vulnerable to human error, and constrained by limited access to records. Digital investigative systems have increasingly replaced or supplemented these processes by enabling biometric verification and centralized retrieval of investigative information.

Within the PNP, AFIS, e-Rogues Gallery, CIRAS, and the e-Warrant System support different but interconnected investigative functions. AFIS supports fingerprint-based identification; e-Rogues Gallery provides digital criminal profiles and photographic references; CIRAS supports the recording, retrieval, and analysis of crime-related information; and the e-Warrant System facilitates verification of active warrants. The NCRPO provides a particularly relevant setting because its five police districts handle a large and complex volume of investigative and intelligence activities.

The study addresses a research gap identified in the dissertation: although prior literature establishes the value of digital policing, comparatively limited empirical work directly links the utilization of specific PNP databases with measurable investigative outcomes while simultaneously examining the lived experiences of investigators and intelligence operatives. The present study therefore integrates quantitative measures of utilization, effectiveness, and relationships with qualitative evidence concerning actual operational conditions.

Purpose and Research Questions

The study aimed to evaluate how digital databases were utilized by the PNP in suspect identification during criminal investigations. Specifically, it sought to determine: (1) the level of utilization of AFIS, e-Rogues Gallery, CIRAS, and the e-Warrant System; (2) the effectiveness of digital database-supported suspect identification in terms of speed, accuracy, and case resolution; (3) the significant relationship between perceived

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

database effectiveness and investigative outcomes; (4) the lived experiences of informants in using the systems; and (5) an appropriate intervention to enhance utilization and investigative effectiveness. The null hypothesis stated that there is no significant relationship between perceived effectiveness of the specific digital databases and suspect-identification outcomes in terms of speed, accuracy, and case resolution.

Theoretical and Conceptual Basis

The study is anchored primarily on the Technology Acceptance Model (Davis, 1989), which explains technology use through perceived usefulness and perceived ease of use. The dissertation also draws on Routine Activity Theory (Cohen & Felson, 1979), Systems Theory, Pragmatism, Empiricism, and Utilitarianism. In the context of the study, digital databases are valuable not merely because they exist, but because personnel can access, trust, and use them to produce timely and accurate investigative information.

The conceptual framework follows an Input–Process–Output orientation. Inputs include the research questions, digital databases, relevant legal and organizational bases, theoretical anchors, and data-gathering instruments. The process consists of quantitative survey administration and statistical analysis followed by qualitative interviews, transcription, coding, and thematic analysis. The output is the Digital Investigative Capability and Resilience Framework (DICRF), with feedback intended to support continuing improvement of policies, systems, and investigative practices.

Significance and Scope

The findings are intended to support PNP leadership, investigators, intelligence and information-technology units, policymakers, and criminology researchers by identifying both strengths and operational gaps in digital investigative systems. The study was conducted within the NCRPO and focused on investigators and intelligence operatives with direct exposure to AFIS, e-Rogues Gallery, CIRAS, and the e-Warrant System.

2. METHODS

Research Design

The study employed an explanatory sequential mixed-methods design. The quantitative phase was conducted first to describe utilization and perceived effectiveness and to test relationships among the variables. The qualitative phase followed to explain and contextualize the quantitative findings through key informant interviews. This sequence allowed numerical patterns to be interpreted alongside the operational experiences of personnel.

Participants and Setting

The population consisted of investigators and intelligence operatives assigned across the NCRPO's five police districts: Manila Police District, Quezon City Police District, Southern Police District, Northern Police District, and Eastern Police District. Because exact operational strength figures were treated as restricted information, the study used an estimated population of 1,450 eligible personnel. Slovin's formula at a 5% margin of error yielded a minimum sample of 313; however, 509 completed and validated questionnaires were obtained. The quantitative sample comprised 298 investigators (58.7%) and 210 intelligence operatives (41.3%). Ten key informants were purposively selected for the qualitative phase based on extensive operational experience and direct involvement in digital case processing and suspect identification.

Research Instruments and Data Collection

Two instruments were used: a researcher-made survey questionnaire and a structured interview guide. The questionnaire covered respondent profile, utilization of AFIS, e-Rogues Gallery, CIRAS, and e-Warrant, and perceived effectiveness in speed, accuracy, and case resolution. The interview guide explored actual system use, facilitating factors, operational challenges, and recommendations. The questionnaire underwent content validation by three experts and pilot reliability testing with 30 PNP personnel outside the actual sample; the dissertation reports Cronbach's alpha of at least 0.70 as the acceptable reliability criterion.

Data collection involved securing institutional permission, coordinating with NCRPO offices and unit heads, administering the survey, conducting structured interviews, documenting responses, and processing quantitative and qualitative data. Informed consent, voluntary participation, confidentiality, anonymity, and secure handling of data were observed. Qualitative responses were transcribed, translated when necessary, coded, and analyzed using the six-phase thematic analysis approach of Braun and Clarke (2006).

Statistical Treatment

Median and interquartile range were used to summarize ordinal responses. A four-point utilization scale interpreted scores from 3.26–4.00 as "Always Utilized," 2.51–3.25 as "Often Utilized," 1.76–2.50 as "Sometimes Utilized," and 1.00–1.75 as "Never Utilized." For effectiveness, 3.26–4.00 was interpreted as "Highly Effective," 2.51–3.25 as "Effective," 1.76–2.50 as "Moderately Effective," and 1.00–1.75 as "Not Effective." Spearman's rho was used for the relationship analysis because the measures were ordinal and did not require normally distributed data. Statistical significance was evaluated at the 0.05 level.

3. RESULTS

Utilization of Digital Databases

The quantitative results demonstrate consistently high utilization across the four digital databases. AFIS was rated Always Utilized by both respondent groups, with an overall median of 3.00 in the dissertation's Table 1. e-Rogues Gallery, CIRAS, and the e-Warrant System each obtained an overall median of 4.00 (Always Utilized) for both investigators and intelligence operatives. The pattern indicates that the systems are embedded in routine investigative and intelligence work.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

Database	Investigators	Intelligence Operatives	Overall Interpretation
AFIS	3.00 – Always Utilized	3.00 – Always Utilized	Always Utilized
e-Rogues Gallery	4.00 – Always Utilized	4.00 – Always Utilized	Always Utilized
CIRAS	4.00 – Always Utilized	4.00 – Always Utilized	Always Utilized
e-Warrant System	4.00 – Always Utilized	4.00 – Always Utilized	Always Utilized

Table 1. Summary of digital database utilization results. Source: dissertation Tables 1–4.

Perceived Effectiveness in Suspect Identification

All three outcome dimensions—speed, accuracy, and case resolution—received a median of 4.00 (Highly Effective) from both investigators and intelligence operatives. For speed, respondents reported that digital databases expedite identification and verification, minimize delays in accessing records, improve timeliness, facilitate faster coordination, and support prompt processing of suspect-related information. For accuracy, respondents reported that the systems improve precision, support reliable decision-making, reduce inconsistencies and errors, strengthen record integrity, and provide accurate evidentiary support. For case resolution, respondents reported that digital databases strengthen case build-up and suspect tracking, facilitate coordination and information exchange, support effective investigative outcomes, and reinforce intelligence efforts leading to case resolution.

Outcome	Investigators	Intelligence Operatives	Interpretation
Speed of identification	4.00	4.00	Highly Effective
Accuracy of identification	4.00	4.00	Highly Effective
Case resolution outcomes	4.00	4.00	Highly Effective

Table 2. Summary of perceived effectiveness results. Source: dissertation Tables 5–7.

Relationship Between Database Effectiveness and Investigative Outcomes

All database-outcome relationships were positive and statistically significant at $p < .001$ ($N = 509$; $df = 507$). The dissertation's Table 8 reports Spearman's rho coefficients ranging from 0.490 to 0.653. AFIS showed moderate positive relationships with speed ($\rho = .490$), accuracy ($\rho = .502$), and case resolution ($\rho = .538$). e-Rogues Gallery showed strong positive relationships with speed ($\rho = .616$), accuracy ($\rho = .653$), and case resolution ($\rho = .638$). CIRAS showed strong positive relationships with speed ($\rho = .599$), accuracy ($\rho = .633$), and case resolution ($\rho = .621$). The e-Warrant System showed strong positive relationships with speed ($\rho = .598$), accuracy ($\rho = .615$), and case resolution ($\rho = .612$). The null hypothesis was rejected.

Database	Speed ρ	Accuracy ρ	Case Resolution ρ	p-value
AFIS	.490	.502	.538	< .001
e-Rogues Gallery	.616	.653	.638	< .001
CIRAS	.599	.633	.621	< .001
e-Warrant System	.598	.615	.612	< .001

Table 3. Spearman rank-order correlations between perceived database effectiveness and investigative outcomes. Source: dissertation Table 8.

Qualitative Results: Lived Experiences

The qualitative phase revealed that high perceived effectiveness coexists with significant operational vulnerabilities. The dissertation's thematic analysis identified sixteen themes. These themes can be read as two broad result clusters: enabling conditions and constraints on digital investigative resilience.

Enabling Experiences

Theme 1. Digital Databases as Tools for Suspect Identification and Information Verification

Theme 2. Digital Database Accessibility as a Facilitator of Investigative Operations

Theme 3. Enhanced Suspect Identification Through Faster Access to Digital Information

Theme 5. Faster Information Retrieval and Streamlined Investigative Processes

Theme 6. Improved Investigative Accuracy Through Accessible and Verifiable Digital Records

Theme 7. Faster Information Retrieval and Streamlined Investigative Processes

Theme 8. Improved Investigative Accuracy Through Accessible and Verifiable Digital Records

Across these themes, informants described digital systems as practical tools for verifying identities, retrieving records, accelerating investigative work, reducing reliance on paper-based searches, and improving the availability of information for case build-up and suspect tracking.

Operational Constraints and Resilience Needs

Theme 4. System Accessibility and Technical Limitations as Constraints in Investigative Work

Theme 9. Dependence on Internet Connectivity and System Reliability in Digital Investigations

Theme 10. Restricted System Access as a Barrier to Efficient Database Utilization

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

Theme 11. Training and Technical Competence as Foundations for Effective Digital Database Utilization
Theme 12. Organizational Policies and Authorized Access as Safeguards for Proper System Utilization
Theme 13. Outdated and Incomplete Records as Barriers to Accurate Suspect Identification
Theme 14. Inaccurate Records as Risks to Investigative Reliability and Case Outcomes
Theme 15. System Interruptions and Delayed Updates as Causes of Investigative Delays
Theme 16. Technical Disruptions as Operational Barriers to Case Resolution and Service Delivery

The informants identified unstable internet connectivity, system downtime, limited access caused by single-user or OTP arrangements, training needs, organizational access policies, outdated photographs and records, inaccurate entries, delayed updates, and the need to revert to manual processes during technical failures. The findings emphasize that system availability and data quality are as important as the existence of the digital platforms themselves.

4. DISCUSSION

The quantitative findings indicate that digital databases have moved beyond optional administrative tools and have become integrated into routine investigative and intelligence operations. The uniform "Always Utilized" ratings across respondent groups suggest broad organizational adoption. This pattern is consistent with the study's Technology Acceptance Model orientation: personnel appear to perceive the systems as useful because they facilitate identity verification, information retrieval, coordination, and investigative decision-making.

The uniformly "Highly Effective" ratings for speed, accuracy, and case resolution further indicate that respondents associate digital database use with improved investigative performance. The findings are consistent with the study's theoretical premise that the practical value of technology is demonstrated through actual operational results. They also reflect the Systems Theory perspective because the benefits of digital investigation depend on the interaction of databases, personnel, infrastructure, access controls, and information quality rather than on software alone.

The correlation analysis provides empirical support for the proposition that higher perceived effectiveness of digital databases is associated with better investigative outcomes. The strongest Spearman relationship in the table was between e-Rogues Gallery and accuracy ($\rho = .653$), while all relationships were positive and highly significant. These results support rejecting the null hypothesis. The correlations should be interpreted as associations rather than proof of causation; nevertheless, the consistent pattern across four systems and three outcomes strengthens the empirical evidence for the operational importance of digital investigative capabilities.

The qualitative findings add an important qualification to the positive quantitative results. Personnel may rate a system as highly effective when it is functioning, yet the same system may become an operational bottleneck when internet connectivity fails, access is concentrated in one designated user, records are outdated, or updates are delayed. Thus, the study reveals a digital-resilience paradox: the PNP has highly utilized digital systems, but their operational value remains vulnerable to infrastructure, access, training, and data-quality failures.

The data-quality themes are particularly important because digital identification is only as reliable as the information available to the system. Outdated photographs, incomplete profiles, typographical errors, and delayed warrant updates may weaken identification and create operational risks. This finding supports the study's emphasis on proactive record maintenance and reinforces the need for secure information sharing that balances operational access with confidentiality and data protection.

The findings also indicate that access expansion should not mean unrestricted access. The informants emphasized a need-to-know approach, authorized access, confidentiality, and accountability. This is consistent with the proposed DICRF, which seeks to replace single-point access bottlenecks with tiered, role-based access while maintaining security safeguards.

Digital Investigative Capability and Resilience Framework (DICRF)

The DICRF was developed from the integration of the quantitative and qualitative findings. Its purpose is to move the PNP from digital adoption toward digital resilience by reducing downtime, preventing access bottlenecks, improving data quality, strengthening personnel competence, and enabling secure information sharing.

Component	Operational Problem Addressed	Core Mechanism
Decentralized Offline Continuity Protocol (DOCP)	Internet instability and system downtime	Encrypted district-level read-only cache of high-priority CIRAS and e-Warrant data with automatic re-synchronization
Multi-Tiered Role-Based Access Expansion (M-TRAX)	Single-user/OTP access bottlenecks	At least three vetted investigators per shift with tiered credentials and role-based access
Proactive Record Purging and Biometric Refresh Drive (PRP-BRD)	Outdated/incomplete suspect records	Automated data-decay flags, updated digital mugshots, and safeguards against duplicate/incorrect records
Specialized Digital Intelligence Competency Certification (SDICC)	Training and technical competence gaps	Advanced database querying, AFIS capture quality, and Data Privacy Act compliance certification
Secure Cross-Jurisdictional Data Bridge (SCDB)	Information silos and access/security tension	Need-to-know, time-limited cross-district information requests with auditable approvals

Table 4. Core components of the proposed Digital Investigative Capability and Resilience Framework.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

The proposed implementation strategy in the dissertation is phased: Months 1–3 focus on policy and software architecture; Months 4–6 on training and access restructuring; and Months 7–12 on pilot testing, full integration, and quarterly auditing. The framework is intended to provide continuity during infrastructure failures while preserving information security and accountability.

5. CONCLUSION AND IMPLICATIONS

Digital databases—AFIS, e-Rogues Gallery, CIRAS, and the e-Warrant System—are essential and extensively utilized tools in suspect identification and police investigations within the NCRPO. Investigators and intelligence operatives consistently perceive these systems as highly effective for improving speed, accuracy, and case resolution. The significant positive relationships across all database-outcome pairs demonstrate that perceived database effectiveness is strongly associated with better investigative outcomes.

At the same time, the qualitative evidence demonstrates that digital adoption does not automatically guarantee digital resilience. Reliable infrastructure, stable connectivity, appropriate access arrangements, technically competent personnel, and accurate and current records are necessary to sustain the benefits of digital investigation. The principal implication is therefore organizational: strengthening investigative technology requires simultaneous investment in systems, people, data governance, access architecture, and continuity mechanisms.

Recommendations

1. Implement the Decentralized Offline Continuity Protocol (DOCP) to maintain access to high-priority investigative information during internet or server outages.
2. Adopt Multi-Tiered Role-Based Access Expansion (M-TRAX) to reduce delays caused by single-user access and OTP bottlenecks while maintaining authorization controls.
3. Institutionalize the Proactive Record Purging and Biometric Refresh Drive (PRP-BRD) to identify and update outdated suspect profiles and improve data accuracy.
4. Deploy the Secure Cross-Jurisdictional Data Bridge (SCDB) to support controlled, auditable information sharing among districts.
5. Require Specialized Digital Intelligence Competency Certification (SDICC) for personnel authorized to use the digital databases, including advanced querying, AFIS capture quality, and data-privacy compliance.
6. Formally adopt and pilot the DICRF across the five NCRPO districts and evaluate its effect on system downtime, access delays, data quality, and investigative continuity.

REFERENCES

1. *Bertalanffy, L. von. (1968). General system theory: Foundations, development, applications. George Braziller.*
2. *Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.*
3. *Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.*
4. *Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.*
5. *Ratcliffe, J. H. (2016). Intelligence-led policing (2nd ed.). Routledge.*
6. *Schmalleger, F. (2020). Criminal justice today: An introductory text for the 21st century (15th ed.). Pearson.*
7. *Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. (2019). Criminal investigation (13th ed.). McGraw-Hill Education.*
8. *Delos Santos, M. G. (2021). Modern investigative techniques in Philippine policing. Manila: Criminology Press.*
9. *Reyes, J. A., & Mendoza, F. L. (2020). Digital policing and database systems. Quezon City: Justice and Safety Publishing House.*
10. *Chan, J. (2001). The technology game: How information technology is transforming police practice. Criminal Justice Press.*
11. *Philippine National Police. (2020). PNP Digital Transformation Roadmap 2020–2030.*
12. *Philippine National Police. PNP Memorandum Circular No. 2010-016.*
13. *Philippine National Police. PNP Memorandum Circular No. 2020-064.*
14. *Philippine National Police. PNP Memorandum Circular No. 2021-004.*
15. *Republic Act No. 6975. Department of the Interior and Local Government Act of 1990.*
16. *Republic Act No. 10175. Cybercrime Prevention Act of 2012.*
17. *Republic Act No. 10173. Data Privacy Act of 2012.*
18. *United Nations. Sustainable Development Goal 16: Peace, Justice and Strong Institutions.*