

International Journal of Advanced Engineering, Management and Science

Journal CrossRef DOI: 10.22161/ijaems

(IJAEMS)

An Open Access Peer-Reviewed International Journal



Vol-9, Issue-4 | Apr 2023

Issue DOI: 10.22161/ijaems.93

International Journal of Advanced Engineering, Management and Science

(ISSN: 2454-1311)

DOI: 10.22161/ijaems

Vol-9, Issue-4

April, 2023

Editor in Chief

Dr. Dinh Tran Ngoc Huy

Chief Executive Editor

Dr. S. Suman Rajest

Copyright © 2023 International Journal of Advanced Engineering, Management and Science

Publisher

Infogain Publication

Email: ijaems.editor@gmail.com ; editor@ijaems.com

Web: www.ijaems.com

Editorial Board/ Reviewer Board

Dr. Zafer Omer Ozdemir

Energy Systems Engineering Kırklareli, Kırklareli University, Turkey

Dr. H.Saremi

Vice- chancellor For Administrative & Finance Affairs, Islamic Azad university of Iran, Quchan branch, Quchan-Iran

Dr. Ahmed Kadhim Hussein

Department of Mechanical Engineering, College of Engineering, University of Babylon, Republic of Iraq

Mohammad Reza Kabaranzad Ghadim

Associated Prof., Department of Management, Industrial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

Prof. Ramel D. Tomaquin

Prof. 6 in the College of Business and Management, Surigao del Sur State University (SDSSU), Tandag City, Surigao Del Sur, Philippines

Dr. Ram Karan Singh

BE.(Civil Engineering), M.Tech.(Hydraulics Engineering), PhD(Hydraulics & Water Resources Engineering),BITS- Pilani, Professor, Department of Civil Engineering,King Khalid University, Saudi Arabia.

Dr. Asheesh Kumar Shah

IIM Calcutta, Wharton School of Business, DAVV INDORE, SGSITS, Indore Country Head at CraftSOL Technology Pvt.Ltd, Country Coordinator at French Embassy, Project Coordinator at IIT Delhi, INDIA

Dr. Ebrahim Nohani

Ph.D.(hydraulic Structures), Department of hydraulic Structures,Islamic Azad University, Dezful, IRAN.

Dr.Dinh Tran Ngoc Huy

Specialization Banking and Finance, Professor,Department Banking and Finance , Viet Nam

Dr. Shuai Li

Computer Science and Engineering, University of Cambridge, England, Great Britain

Dr. Ahmadad Nabih ZakiRashed

Specialization Optical Communication System,Professor,Department of Electronic Engineering, Menoufia University

Dr.Alok Kumar Bharadwaj

BE(AMU), ME(IIT, Roorkee), Ph.D (AMU),Professor, Department of Electrical Engineering, INDIA

Dr. M. Kannan

Specialization in Software Engineering and Data mining, Ph.D, Professor, Computer Science,SCSVMV University, Kanchipuram, India

Dr.Sambit Kumar Mishra

Specialization Database Management Systems, BE, ME, Ph.D, Professor, Computer Science Engineering Gandhi Institute for Education and Technology, Baniatangi, Khordha, India

Dr. M. Venkata Ramana

Specialization in Nano Crystal Technology, Ph.D,Professor, Physics,Andhara Pradesh, INDIA

Dr.Swapnesh Taterh

Ph.d with Specialization in Information System Security, Associate Professor, Department of Computer Science Engineering Amity University, INDIA

Dr. Rabindra Kayastha

Associate Professor, Department of Natural Sciences, School of Science, Kathmandu University, Nepal
Amir Azizi

Assistant Professor, Department of Industrial Engineering, Science and Research Branch-Islamic Azad University, Tehran,Iran

Dr. A. Heidari

Faculty of Chemistry, California South University (CSU), Irvine, California, USA

DR. C. M. Velu

Prof. & HOD, CSE, Datta Kala Group of Institutions, Pune, India

Dr. Sameh El-Sayed Mohamed Yehia

Assistant Professor, Civil Engineering (Structural), Higher Institute of Engineering -El-Shorouk Academy, Cairo, Egypt

Dr. Hou, Cheng-I

Specialization in Software Engineering, Artificial Intelligence, Wisdom Tourism, Leisure Agriculture and Farm Planning, Associate Professor, Department of Tourism and MICE, Chung Hua University, Hsinchu Taiwan

Branga Adrian Nicolae

Associate Professor, Teaching and research work in Numerical Analysis, Approximation Theory and Spline Functions, Lucian Blaga University of Sibiu, Romania

Dr. Amit Rath

Department of ECE, SEEC, Manipal University Jaipur, Rajasthan, India

Dr. Elsanosy M. Elamin

Dept. of Electrical Engineering, Faculty of Engineering. University of Kordofan, P.O. Box: 160, Elobeid, Sudan

Dr. Subhaschandra Gulabrai Desai

Professor, Computer Engineering, SAL Institute of Technology and Engineering Research, Ahmedabad, Gujarat, India

Dr. Manjunatha Reddy H S

Prof & Head-ECE, Global Academy of Technology, Raja Rajeshwari Nagar, Bangalore , India

Herlandí de Souza Andrade

Centro Estadual de Educação Tecnológica Paula Souza, Faculdade de Tecnologia de Guaratinguetá Av. Prof. João Rodrigues Alckmin, 1501 Jardim Esperança - Guaratinguetá 12517475, SP – Brazil

Dr. Eman Yaser Daraghmi

Assistant Professor, Ptuk, Tulkarm, Palestine (Teaching Artificial intelligence, mobile computing, advanced programming language (JAVA), Advanced topics in database management systems, parallel computing, and linear algebra)

Ali İhsan KAYA

Head of Department, Burdur Mehmet Akif Ersoy University, Technical Sciences Vocational School Department of Design,Turkey

Professor Jacinta A.Opara

Professor and Director, Centre for Health and Environmental Studies, University of Maiduguri, P. M.B 1069, Maiduguri Nigeria



Siamak Hoseinzadeh

Ph.D. in Energy Conversion Engineering

Lecturer & Project Supervisor of University, Level 3/3, Islamic Azad University West Tehran Branch, Tehran, Iran.

Vol-9, Issue-4, April, 2023

(DOI: 10.22161/ijaems.94)

<i>Sr No.</i>	<i>Title with Article detail</i>
<i>1</i>	<i>Evaluating Network Forensics Applying Advanced Tools</i> <i>Abdullah Shah</i>  <i>DOI: 10.22161/ijaems.94.1</i> <i>Page No: 01-09</i>
<i>2</i>	<i>Behavior of Composite Piles Reinforced by Geosynthetics</i> <i>El-Sayed A. El-Kasaby, Mohab Roshdy, Mahmoud Awwad, Mona I. Badawi</i>  <i>DOI: 10.22161/ijaems.94.2</i> <i>Page No: 10-19</i>

Evaluating Network Forensics Applying Advanced Tools

Abdullah Shah

engabdullah838@gmail.com

Received: 24 Feb 2023; Received in revised form: 18 Mar 2023; Accepted: 25 Mar 2023; Available online: 03 Apr 2023

Abstract— Network forensics comes under the domain of digital forensics and deals with evidences left behind on the network after a cyber-attack. It is indication of the weakness that led to the crime and the possible cause. Network focused research comes up with many challenges which involves the collection, storage, content, privacy, confiscation and the admissibility. It is important and critical for any network forensic researcher or the investigator to consider adopting efficient forensic network investigation framework or the methodologies in order to improve investigation process. The main aim of this research contribution was to do a comprehensive analysis of concepts of networks forensics through extensive investigation and by analyzing various methodologies and associated tools which should be used in the network forensic investigations. Detailed and in depth analysis of concepts of network forensic investigation on a designed/conceived network architecture was carried out which was then followed by analyzing various methodologies and tools employed. An innovative framework for the investigation was designed which can be used by any forensic expert. The acquired data was analyzed by using information, strategizing and collecting evidence and by analyzing and reporting of the methodologies on the conceptualized network. Consequently, it led to the researcher to adopt and utilize a powerful and efficient forensic network methodology that will ultimately help in improving the investigation process and providing required tools/techniques along with the requisite guidelines that will determine the approach, methods, and strategies which are to be used for network forensic process to be followed and be executed with the use of relevant tools that will tend to help in the simplification and improvement of the forensics investigation process.

Keywords— Forensic Science, Network Forensics, OSCAR.

I. INTRODUCTION & BACKGROUND

In this section, the author presents introduction and the chosen topics background relating to Network Forensics and various concepts pertaining to it including the advanced tools being used to achieve this.

1.1. Introduction & Background

The Digital forensic and subsequently the network forensics stems from the forensic science with its evolution shown below;

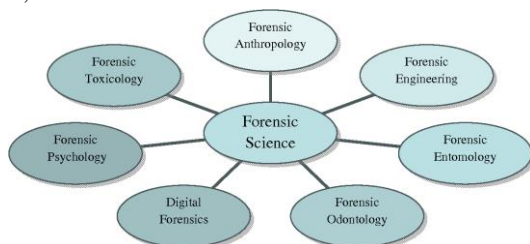


Fig.1.1: Forensic Science Branches

The forensic science has many sub-branches which are shown in the figure above and for each of them the advanced research is being carried out by the field researchers. Figure below shows in more detail how the forensic science has penetrated in every walk of life.

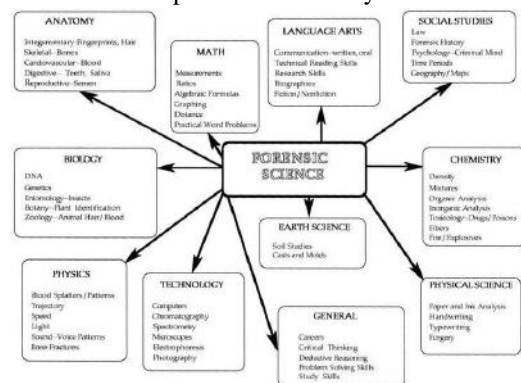


Fig.1.2: Forensic Science Penetration

Network forensics falls under the category of (DF) related to monitoring and analyzing computer network traffic for data collection purposes. Unlike DF, network forensic deals with dynamic information. It comes under the domain of DF and is related to the investigation of evidence left on the network following any cyber-attack. This forensic allowed the businesses to make it possible to enhance their security situation and apply the requisite corrections appropriately. In fact, network forensics is a subset of the digital forensics itself is a branch of intelligence science - where jurists look for technologies or data that contain criminal evidence. Network forensics, surprisingly, refers to the investigation and analysis of all network traffic suspected of cybercrime i.e. proliferation of malicious software that steals data.

Law enforcement agencies use network forensics to analyze network traffic data collected from suspected criminal activities. Analysts will search for data that identifies human interactions, file fraud, and through use of keywords. By the use of network and digital forensics, the law enforcement agencies and the crime investigators can track communications and can easily set up time-based network events installed through a network controlled system.

In addition to criminal investigations, network forensics is often used to analyze network events in order to trace the origins of robberies and other security-related incidents. This includes looking at suspected network locations, collecting information about network features and resources & identifying incidents of unauthorized network access.

There exist 2 methods for full network forensics;

1. "Catch as much as possible" method: Capturing network traffic for analysis requiring long process and maintenance.
2. Stop, watch and listen method: Based on analyzing each data packet which passes across network only what looks like suspicious and worthy of analysis data thus needing lots of processing power but can be achieved by less storage space.

Unlike DF, network forensics are much harder to perform as data transferred across the network and then lost; in CF data is usually stored on disk or solid state storage which makes them easy to access.

The applications of Digital Forensics are shown below;



Fig.1.3: Applications of Digital Forensics

The subsequent domains falling under them are shown in the figures below.

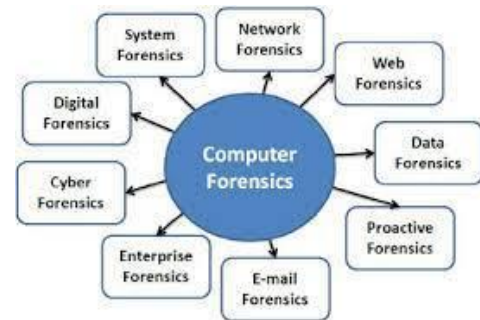


Fig.1.4: Computer Forensics



Fig.1.5: Mobile Forensics

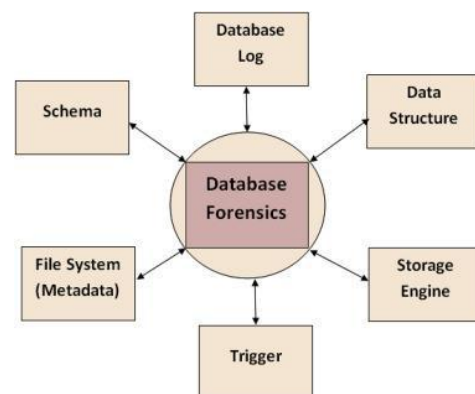


Fig.1.6: Database Forensics



Fig.1.6: Live Forensics

And finally the Network Forensics and its challenges, being the focus of this research contribution.

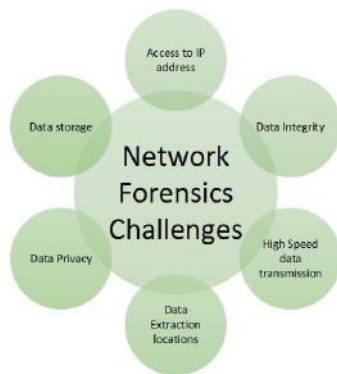


Fig.1.7: Network Forensics

Investigative process includes:

- I - Identification
- P - Preservation
- C - Collection
- E - Examination
- A - Analysis
- P - Presentation

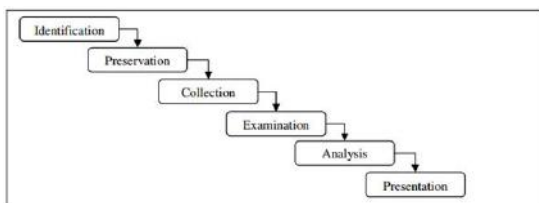


Fig.1.8: Network Forensics Investigative Process

Identifying attack patterns requires understanding of applications and network protocols.

- Protocols (on the web)
- FTP - File Transfer Protocols
- E-Mail (Protocols)
- Network (Protocols)

Application-Specific Digital Forensics Investigative Model is shown below;

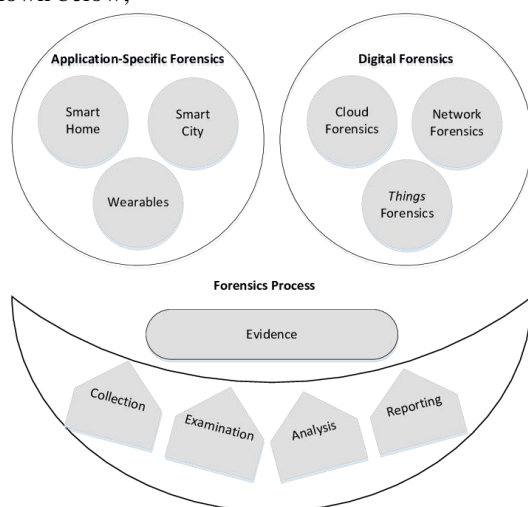


Fig.1.8: Digital Forensics Investigative Model

Network Forensics Tools include;

- Wireshark
- Tshark
- Dumpcap
- Network Forensic Analysis Tools

The requisite features are shown in the below figures.



Fig.1.9: Wireshark Features

(Source: <https://www.wireshark.org/>)

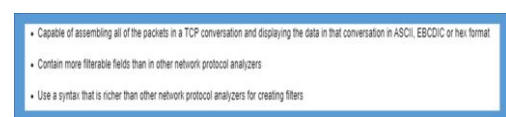


Fig.1.10: Tshark Features [25]

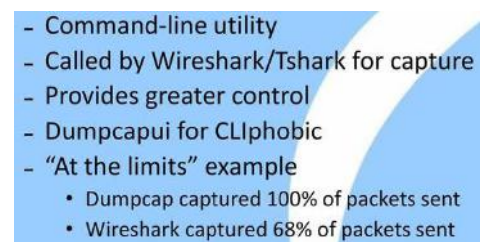


Fig.1.11: Dumpcap Features

(Source: <https://docplayer.net/10961126-13-maximizing-packet-capture-performance-andrew-brown.html>)

Name	Platform	Description
Paraben Netanalysis	Windows	It interrogates the Web browser cache and history data with powerful searching, filtering, and evidence identification.
LogLogic's LX 2000	Windows	It is a log analysis tool. It ingests and processes all log files to secure, monitor and manage the IT environment. It dramatically reduces the time and cost required to uncover the information.
Webtracer	N/A	It determines the Owner of the website, the location of the server, the sender of an email, and other evidence of internet identity.
Spector CNE	Windows and Linux	It records everything the employees do online, including IM (instant messengers), chats, sending and receiving e-mails, visiting websites, launching applications, downloading files, and typing keys.
dtSearch	Windows	It searches terabytes of text across a desktop, network, Internet or intranet sites. It consists of special forensic search options. It supports public and secure, static and dynamic web data.

Fig.1.12: Network Forensic Analysis Proprietary Tools

(Source:

https://www.researchgate.net/figure/Proprietary-tools-for-Network-Forensics_tbl6_315726562)

1.2. The Research Problem

Not adhering to digital forensics can lead to organizations losing continuity and the availability of core services. Vulnerabilities can multiply in the networks making it vulnerable thus compromising security issues. This can lead to the collapse of all communication mechanisms because of network nodes failures and the whole setup can be compromised by the intruding hacker.

1.3. The Purpose of the Study

Penetration of brings many challenges associated with security and data breaches. Cyber attacker's come up with extremely complicated means of infiltrating networks' security. Hence the expert administrator monitoring the network activities should be fully equipped to identify the security vulnerabilities and can capture cyber related offenders. The main purpose of this research contribution is to come up with a standard and innovative framework which can help in analysis of concepts of networking forensic and the methodologies and associated tools which are to be used for network forensics. This is backed by detailed and exhaustive literature review.

1.4. Objectives

1. Detailed insight into the concept of network forensic investigation on conceptualized network.
2. Analyzing various methodologies-tools which can be used for network forensics.
3. Analyzing data using "obtain information, strategize, collect evidence, analyze and report" (OSCAR) methodology on the conceived network.
4. Designing of an innovative OSCAR Framework

1.5. The Research Questions

1. What are the concept of network forensic investigation and how are they analyzed on the network?
2. What are the best methodologies-tools?
3. How to apply methodology of obtaining information, strategizing, collecting evidence, analyzing and reporting data on a conceived network architecture design?
4. How to design an innovative OSCAR Framework?

1.6. Contribution to Knowledge (Academic)

Contribution of this research relates to providing an analysis which is based on the study of relevant literature. The knowledge helps the researchers to investigate processes which help in cyber-forensics by obtaining, analyzing, evaluating, categorizing, and identifying crucial evidences.

1.7. Statement of Significance (Practical Contribution)

The practical contribution relates to making it possible to apprehend a cyber-criminal. It is achieved through using effective forensic network investigation methodologies. The researched upon methodology will provide forensic specialist with essential tools that will determine the approach for obtaining, strategizing, collecting, analyzing

and reporting the findings of a network forensics investigation. It will also identify the network forensic tools for forensics investigation processes.

II. Literature Review

Here, literature review and the gaps are identified in the light of the reviewed publications.

2.1. Literature Review

Nature and type of crime calls for affected victims help [1]. In some cases, Committed computer crime is not the only source of revenue losses but may make the affected organization inoperable. So, it is important to have a way of doing it the necessary research and auditing for the study once and for all associated computer criminals. Kumongo of cyber-criminal investigation, method referred to as network forensics. Network forensics is a process that involves computer research, analysis to find important information that helps in arrest of cybercriminals [2].

It is important to be careful that any provided network is connected to the internet accustomed to various cyber-attack. Attacks are common designed in way that they exploit weaknesses of anything in network. The investigator is therefore assigned a task the burden of coming up with strategies that are important to do network forensic process for diagnosis network entry conditions [3].

Idea of protecting trade secrets has been adopted with new significance as information with an independent economy or competitive value [5]. One of the many trade problems secrets produce important and sensitive information such as the result of increased information and communication space the exchange is a widespread response to government in the use of forcing steel with strong obstacles results, as in the case of Terry [6]. This is an in-depth study referenced at [7], [8], [9], [10], [11].

Almulhem added that network forensics are highly correlated with the security model. The network (digital forensics) emphasizes the design and implementation of methods, tools, and concepts aimed at improving forensic investigation process [12]. Kilpatrick et al. proposes the implementation of SCADA (monitoring control and constructive data acquisition programs an important infrastructure for network forensics [13]. It also plays a key role in implementation of machine-to-machine safety methods networks [14].

It is important to review several cases subjects where the concept has been used sufficiently. In particular, Kurniawan and Riadi [15] were able to test again use the unique framework from which it was obtained use the concept of network forensics analysis once point to the behavior of the infamous Cerber Ransomware. As noted by Messier and Bensefia and Ghoualmi, most fire protection systems have the ability to use software power in UNIX/Windows platforms [16] [17].

It is noteworthy that most Honeypot services are secretive [18]. Honey jars are considered important components which help to improve organizational safety [19]. Network forensics is different from access by the evidence gathered must be accepted in court as well hence satisfying technical/legal concerns [20].

While the acquisition of intervention helps in improving computer network security, network forensics are key corresponding to the need to identify related evidence security breach. Network forensics is helpful resolving issues related to online terrorism, child pornography, drugs, national security, cybercrime, and corporate intelligence, among others [21] [22] [23].

2.2. Literatures Gaps

There is a need to develop some tools that can parse varied network protocols in place or embedded in different networks. As most of the information carried on the networks is volatile, it is essential that it should be preserved in order to expedite the forensic process.

III. RESEARCH METHODOLOGY AND FRAMEWORK

This section deals with the research methodology and conceptualized framework of this research used by the researcher.

3.1. Research Methodology

After going through the detailed literature review, the research selected the base paper [24]. This research contribution is based on following a comprehensive process which will be executed by using OSCAR (obtain, strategize, collect, analyze and report) principles.



Fig. 3.1: OSCAR

The research will follow the following steps.

- Network Conceptualization

- Identification of Malicious Activities
- Identifying the Source of Activity
- Application of Tools
- Decision Making based on Data Analysis

The designed network will be analysed using the following tools.

- **Wireshark**

Wireshark packet analyser: network troubleshooting, analysis, software and communications protocol development.

- **Tshark**

TShark network protocol analyser: Captures packet data from a live network.

- **Dumpcap**

Dumpcap is network traffic dump tool: Captures packet data from a live network & writes them to file.

- **Network Forensic Analysis Tools (NFATs)**

NFATs help administrators monitor their environment for anomalous traffic, perform forensic analysis and get a clear picture of their environment.

The focus of this research contribution is cantered towards the need to find and look at the malware affecting network hosts. The analysis of the network behaviour can come up with infections, exploited channel, and the payload with ransomware. As we are focussed on the network forensics, hence, in order to move forward, the forensic mechanisms need to be looked at which fall under the following categories.

- Network Security Forensic Mechanisms
 - Embedding the Firewall forensics in the network.
- Honeypot Forensics
 - Network system designed is such to allure by depicting information as critical and sensitive.

A typical firewall forensics scenario is shown in the below figure. The firewall has to detect and mitigate the threat from the attacker using the IPs as identifiers.

A typical honeypot deployment is shown in the below figure. The honeypot is placed between the internet network and the firewall and the attacker instead of breaking the firewall is allured towards the honeypot considering it as the main network server. This saves the other network servers from being attacked and compromised.

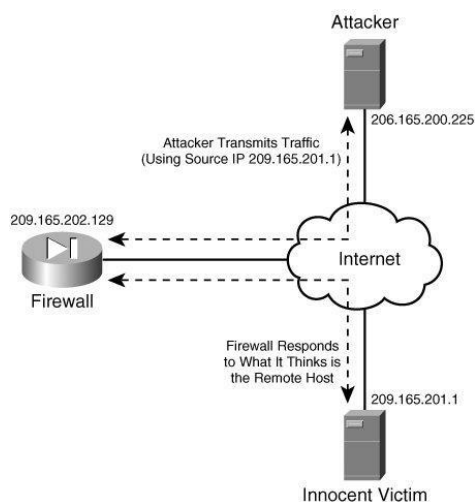


Fig.3.2: Firewall Forensics

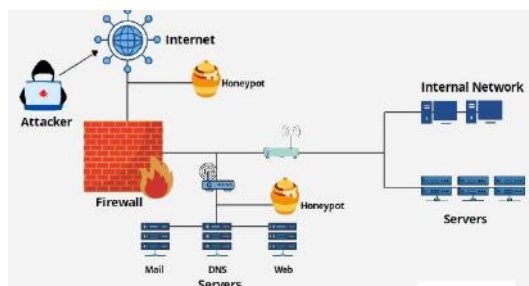


Fig.3.3: Honeypot Forensics (Placement in Network)

Exploring and investigating of network forensics will be done in this research work with identifying a malicious activity, evidence collections and its preservation. This will be followed by evidence reporting and making the decision based on the analysis. All the processes of network forensics will follow the following procedure of OSCAR principle as explained previously in this section. The evidence will be retrieved from the selected network and computing devices. The selected devices are shown in the table below.

Table 3.1: System Designed

S/NO	DESCRIPTION	TYPE OF FORENSICS
1	Application	Internet Browser, E-Mail, Registry, Software, Virus, Worm, Trojans and slack, erased, swap files
2	Deployed System	UNIX, Windows, Log and Audit System
3	Hardware	Personal Computer, Personal Digital Assistant, Printer, Router, Switches, Firewall, Intrusion Detection System
4	Processing	Type: Victim (Client), intermediate, and attacker (Hacker or the Threat Actor)

This will be followed by source of evidence, value, effort, volatility and priority of web proxy cache, firewall logging data and the address resolution protocol tables used for storing the information discovered. Address resolution protocol cache helps the attackers hide behind the fake IP address. Operations systems audit trail, system event logs,

This article can be downloaded from here: www.ijaems.com

applications events logs, alerts logs, recovered data, and swap files of attacker/victim side will be analysed in addition to traffic data packets, firewall log, intrusion detection system log, router log, and access control log of the intermediate devices.

Below innovative conceptualized model is designed by the researcher.

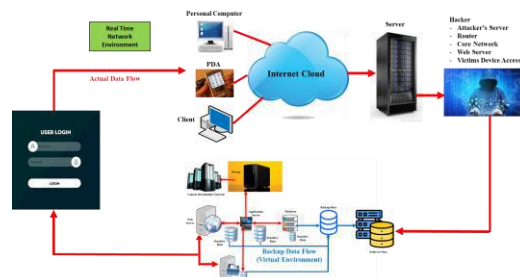


Fig.3.4: Conceptualized Model

In the above conceptualized network design, honeypot devices (sensitive data) is placed in a network for making it possible to carry out a detailed analysis of network activities and the logs being carried throughout the honeypot devices. Hence they are in a good position to help in finding out attacker's logs and activities. The attacker will attack the network and with honeypot devices strategically placed in the network, his attack activities will be logged.

IV. DATA ANALYSIS

The conceptualized network design is discussed in detail in the section after using various tools to capture the attacker's activities.

4.1. OSCAR Framework Design

OSCAR Design Steps are followed in this phase. There are summarized below for clarity.

- Obtaining Information
 - Information regarding the incident
 - Environment
 - Time/Date
 - Discovery
 - Systems involved
 - People involved
 - Devices involved
 - Actions executed after the discovery
 - Discussions record
 - Legal issues
 - Business model
 - Available resources
 - Communication system
 - Network topology
 - Procedures
 - Processes
 - Incidence response management

- Strategizing
 - Investigation goal
 - Investigation time frame
 - Investigation plan
 - Value/Cost of obtaining evidence
 - Evidence acquiring mechanisms
 - Proof acquisition
 - Source
 - Effort required
 - Volatility
 - Expected value
 - Evidence prioritization
 - Data retention policy
 - Access policy
 - Configurations policy
 - Collecting Evidence
 - Obtaining evidence
 - Using reliable and reputable tools
 - Documenting
 - Capturing
 - Store/Transport
 - Security of information
 - Analyzing Evidence
 - System files log
 - Resources log
 - Date, time and source of incident
 - Investigating officer profile
 - Methods used to acquire evidence
 - Devices accessed
 - Custody chain
 - Data/network traffic packets repository
 - Application of forensic tools
 - Storing/transport of log data
 - Reporting
 - Technical information
 - Defensible details
 - Results
- For capturing, filtering and analyzing network traffic
 - Tshark
 - Data network protocol analyzer used for capturing and reading traffic data from live data network from packetized data files.
 - Dumpcap
 - Network traffic analysis is done through the use of this tool which is designed to capture the data packets.
 - Network Forensic Analysis Tools
 - Used for tracking networks and gathering malicious traffic information

4.3. Data Analysis

The conceptualized network is implemented using the tools outlined in the previous section. The below table outlines the setup details.

Table 4.1: Design Setup

S/NO	ATTRIBUTE	DETAILS
1	Source of Evidence	Web Proxy Cache, Firewall logs, Address Resolution Protocol Tables
2	Affiliation	End side - attacker and/or victim side (Operation system audit trail, system event log, application event log, alert log, recovered data, and swap files), Intermediate (Traffic data packets, firewall log, IDS log, router log, and access control log)
3	Device/Tool	Laptop-1 (Usage: Creating test network & host proxies) iPad (Usage: Test device connected to test network) Proxy (Usage: Capture/save live network traffic) Wireshark (Usage: Capture/save live network traffic) Burp Suite (Usage: Capture live network traffic) Laptop-2 (Usage: Network forensics of iOS apps) Network Miner (Usage: Analyze network traffic)

During the process of collection of network-based evidence, special care was done pertaining to the collection, storage, content, privacy, confiscation and admissibility. Test network was designed on laptop-1 in addition to the host proxies. The testing was done using iPad as the testing device. The proxy was used to capture the live network traffic. Capturing and saving of the network traffic was achieved through the usage of Wireshark tool and the burp suite. Burp

Suite is used to set up a proxy which allows to test web architecture by routing web traffic through it. Network forensics were collected from the applications on Laptop-2 while the analysis of the network traffic was done using the network miner. The below figures show the stepwise processes.



Fig.4.1: Designed Framework

4.2. Selected Tools

The following tools were selected for the analysis of the conceptualized network along with their functionalities used.

- Wireshark

This article can be downloaded from here: www.ijaems.com

©2023 The Author(s). Published by Infogain Publication.

This work is licensed under a Creative Commons Attribution 4.0 License. <http://creativecommons.org/licenses/by/4.0/>

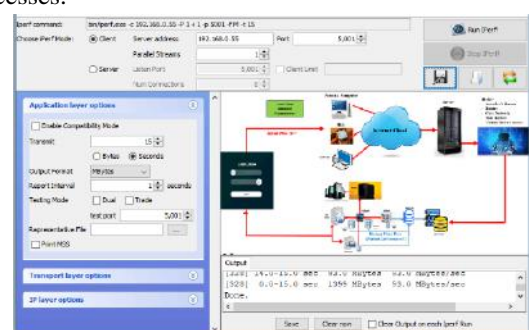


Fig.4.2: Test Network Design

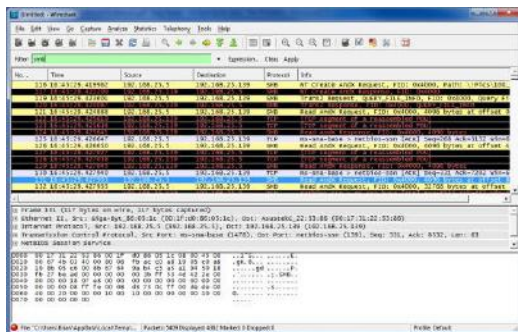


Fig.4.3: Capturing Traffic using Wireshark Tool

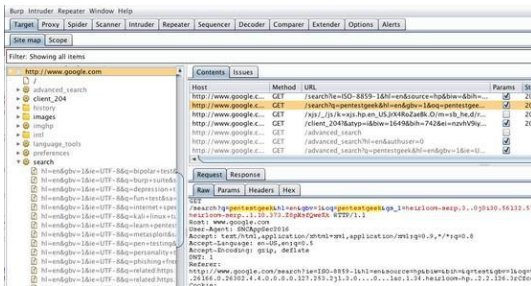


Fig.4.4: Penetration Testing with Burp Suite & Wireshark (Uncovering Vulnerabilities)

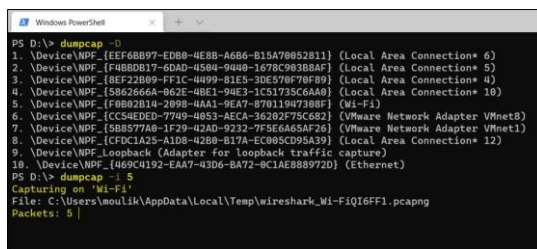


Fig.4.5: Dumpcap to Capture Data Packets

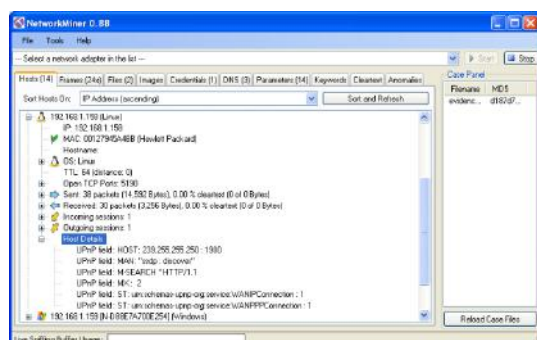


Fig.4.6: Network Miner for Analysis of Network Traffic

V. CONCLUSIONS AND FUTURE RECOMMENDATIONS

The section looks at the conclusions of the research and the future recommendations.

5.1. Conclusions

Following are the outcomes and conclusions of this research contribution.

- Detailed analysis of network forensic investigation on a conceptualized network.
- Methodologies/tools used were analysed and studied in depth.
- Analysed the data using “obtain information, strategize, collect evidence, analysing and reporting (OSCAR) methodologies on the conceived network.
- Designed an innovative OSCAR Framework which can be adopted in any network forensic analysis implementations.
- It was found that Network forensic science is extremely essential important and it helps a cyber-forensics investigator to;
 - O - Obtain
 - A - Analyse
 - E - Evaluate
 - C - Categorize
 - I - Identify crucial evidences
- Helps in apprehending cyber-criminals
- Network forensics investigator should adopt and utilize efficient forensic network investigation methodologies
- OSCAR methodology equips forensic investigator with critical tools and guidelines to develop;
 - Approach
 - Methods
 - Strategies
 - Strategizing
 - Collecting
 - Analysing
 - Report of findings
- Network forensics expert should use top of the line tools.

5.2. Future Recommendations

Following are the recommendations for future research work.

- Development tool kits which can analyse varied network protocols.
- Preserve and document data selectively in advance to speed up the forensic process.

- [1] M. Matsalu et al., "Digitaalse ekspertise t       p  devuse arendamine eestikaitseliidu n  aitel," Ph.D. dissertation, 2019.
- [2] G. S. Chhabra and P. Singh, "Distributed network forensics framework: A systematic review," *International Journal of Computer Applications*, vol. 119, no. 19, 2015.
- [3] G. A. Pimenta Rodrigues, R. de Oliveira Albuquerque, F. E. Gomes de Deus, G. A. De Oliveira J  nior, L. J. Garc  ia Villalba, T.-H. Kim et al., "Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection," *Applied Sciences*, vol. 7, no. 10, p. 1082, 2017.
- [4] D. Chang, M. Ghosh, S. K. Sanadhya, M. Singh, and D. R. White, "Fbhash: A new similarity hashing scheme for digital forensics," *Digital Investigation*, vol. 29, pp. S113–S123, 2019.
- [5] L. Liebler, P. Schmitt, H. Baier, and F. Breitingner, "On efficiency of artifact lookup strategies in digital forensics," *Digital Investigation*, vol. 28, pp. S116–S125, 2019.
- [6] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *Journal of information security and applications*, vol. 40, pp. 217–235, 2018.
- [7] F. Akhtar, J. Li, M. Azeem, S. Chen, H. Pan, Q. Wang, and J.-J. Yang, "Effective large for gestational age prediction using machine learning techniques with monitoring biochemical indicators," *The Journal of Supercomputing*, pp. 1–19, 2019.
- [8] J. Li, D. Zhou, W. Qiu, Y. Shi, J.-J. Yang, S. Chen, Q. Wang, and H. Pan, "Application of weighted gene co-expression network analysis for data from paired design," *Scientific reports*, vol. 8, no. 1, pp. 1–8, 2018.
- [9] F. Akhtar, J. Li, Y. Pei, A. Imran, A. Rajput, M. Azeem, and Q. Wang, "Diagnosis and prediction of large-for-gestational-age fetus using the stacked generalization method," *Applied Sciences*, vol. 9, no. 20, p. 4317, 2019.
- [10] A. Imran, J. Li, Y. Pei, J.-J. Yang, and Q. Wang, "Comparative analysis of vessel segmentation techniques in retinal images," *IEEE Access*, vol. 7, pp. 114 862–114 887, 2019.
- [11] J. Li, L. Liu, J. Sun, H. Mo, J.-J. Yang, S. Chen, H. Liu, Q. Wang, and H. Pan, "Comparison of different machine learning approaches to predict small for gestational age infants," *IEEE Transactions on Big Data*, 2016.
- [12] A. Almulhem, "Network forensics: Notions and challenges," in 2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). IEEE, 2009, pp. 463–466.
- [13] T. Kilpatrick, J. Gonzalez, R. Chandia, M. Papa, and S. Shenoi, "An architecture for scada network forensics," in IFIP International Conference on Digital Forensics. Springer, 2006, pp. 273–285.
- [14] K. Wang, M. Du, Y. Sun, A. Vinel, and Y. Zhang, "Attack detection and distributed forensics in machine-to-machine networks," *IEEE Network*, vol. 30, no. 6, pp. 49–55, 2016.
- [15] A. Kurniawan and I. Riadi, "Detection and analysis cerber ransomware based on network forensics behavior."
- [16] R. Messier, *Network forensics*. John Wiley & Sons, 2017.
- [17] H. Bensefia and N. Ghoulmi, "An intelligent system for decision making in firewall forensics," in *International Conference on Digital Information and Communication Technology and Its Applications*. Springer, 2011, pp. 470–484.
- [18] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Realtime and forensic network data analysis using animated and coordinated visualization," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*. IEEE, 2005, pp. 42–49.
- [19] Q. Al-Mousa and Z. Al-Mousa, "Honeypots aiding network forensics: Challenges and notins," *Journal of Communication*, vol. 8, no. 11, pp. 700–707, 2013.
- [20] J. Llano Tejera, "Herramientas forenses para la respuesta a incidentes inform  ticos," Ph.D. dissertation, Universidad Central "Marta Abreu" de Las Villas, 2014.
- [21] W. Ren, "Modeling network forensics behavior," *Journal of Digital Forensic Practice*, vol. 1, no. 1, pp. 57–65, 2006.
- [22] S. Davidoff and J. Ham, *Network forensics: tracking hackers through cyberspace*. Prentice hall Upper Saddle River, 2012, vol. 2014.
- [23] J. Buric and D. Delija, "Challenges in network forensics," in 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2015, pp. 1382–1386.
- [24] Qureshi, Sirajuddin & Tunio, Saima & Akhtar, Faheem & Wajahat, Ahsan & Nazir, Ahsan. (2021). *Network Forensics: A Comprehensive Review of Tools and Techniques*. *International Journal of Advanced Computer Science and Applications*. 12. 2021. 10.14569/IJACSA.2021.01205103.
- [25] Oracle (2019). *Analyzing Network Traffic with TShark and Wireshark*. Oracle Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle   Solaris 11.3

Behavior of Composite Piles Reinforced by Geosynthetics

El-Sayed A. El-Kasaby^{1a}, Mohab Roshdy^{1b}, Mahmoud Awwad^{1c}, Mona I. Badawi^{1*}

Civil Engineering Department Benha Faculty of Engineering, Benha University, Cairo, Egypt

^a Prof. of soil mechanics and foundations. Email. Profkassaby@gmail.com

^b Lecturer. Email. Mohab.elashmouny@bhit.bu.edu.eg

^c Lecturer. Email. mahmoud.awad@bhit.bu.edu.eg

* Teaching Assistant. PhD Student. Email. Mona.ibrahim@bhit.bu.edu.eg

Received: 15 Mar 2023; Received in revised form: 10 Apr 2023; Accepted: 18 Apr 2023; Available online: 26 Apr 2023

Abstract— This study presents the results of five reinforced concrete (RC) pile specimens that were created and horizontally loaded. The RC piles were reinforced by composite materials such as geogrid, geogrid with a core of steel rod, and geogrid with a core of glass fibre reinforced polymers (GFRP) or carbon fiber reinforced polymers (CFRP) rod. This research is expected to investigate the behavior of using composite materials in pile reinforcement and check their efficiency in carrying horizontal loads. The horizontal pile loading test was applied to four pile specimens and a reference pile specimen reinforced by steel rods. All specimens have the same dimensions (150 mm in diameter and 1050 mm in height). A comparison has been carried out between the experimental results for all specimens and the reference specimen. The experimental results illustrated that the specimens carried a lower ultimate horizontal load by 44%–87% compared to the reference specimen. Also, a non-linear finite element analysis has been verified by Abaqus software and achieved a great degree of reconciliation compared to the experimental results. Finally, a comparison of the reinforcement costs for the specimens revealed that utilizing these composite piles could reduce the cost up to 15.2%.

Keywords— Geosynthetics Geogrid, Composite piles, Horizontal load

I. INTRODUCTION

In recent years, a relatively new trend in deep foundations is the use of composite piles due to their inherent advantages over traditional piles. Composite piles refer to alternative pile foundations composed of fiber reinforced polymers (FRPs) or geosynthetic that are placed into the ground to support axial and horizontal loads [1]. Geosynthetics geogrids was proved to be a promising material in replacing traditional pile materials such as concrete and steel. Development and use in other industries have driven the price of production down to an attractive price point and produced a commercially viable technology [2]. Composite piles with fiber-reinforced polymers (FRP) are a suitable solution to the problems faced by traditional piles as illustrated in several studies [3-13]. Omar Alajarmeh et al. (2020) investigated the use of glass fiber reinforced polymer (GFRP) rods as a solution for corrosion and the use of hollow composite reinforced sections (HCRSSs) to confine the inner concrete

wall in HCCs [14]. AlAjarmeh O.S. et al. (2019) explored the use of GFRP composite rods as reinforcement for HCCs and evaluated the effect of the reinforcement ratio on HCC structural behavior. Their results showed that increasing the diameter and number of rods enhanced the strength, ductility and confinement efficiency of HCC. For columns with equal reinforcement ratios, using more and smaller-diameter GFRP rods yielded 12% higher confinement efficiency than in the columns with fewer and larger-diameter rods. The crushing strain of the GFRP rods embedded in the HCC was 52.1% of the ultimate tensile strain [15]. Previous studies related to the performance of hollow FRP piles only include superficial consideration of the impact behavior of the fiber materials and do not systematically describe their impact strength. These studies described the impact behavior of the fiber composite materials through the observed damage mechanisms only [16][17]. Ahmed H. Ali et al. (2020) presented a numerical analysis investigation, using finite element model (FEM)

and modified compression field theory (MCFT), which was conducted to evaluate the shear capacity and behavior of circular concrete piles reinforced with steel and FRP rods by considering shear behavior, shear strength, and deflection shape [18]. Pando et al. (2006) carried out a large-scale pile load test investigating the performance of FRP piles as the supporting structure for a highway overpass in Virginia. They compared driven precast concrete piles to concrete in-filled FRP piles. Axial pile load tests showed that the FRP piles performed comparably to the concrete pile [19].

This study targeted to examine a new technique for reinforcing piles by using different materials and check their efficiency under horizontal loads(H). horizontal pile loading tests was applied on five piles as reference concrete pile (PSH) reinforced by steel rods, a concrete pile (PGH) reinforced by geosynthetics geogrids (G), and concrete piles (PSGH, PLGH, PCGH) reinforced by geosynthetics geogrids with a core of steel rod in the middle. Also, the costs of the specimens were compared.

Nomenclature	
<i>P</i>	<i>pile</i>
<i>S</i>	<i>steel rod</i>
<i>L</i>	<i>glass fiber rod</i>

<i>C</i>	<i>carbon fiber rod</i>
<i>G</i>	<i>geogrid</i>
<i>H</i>	<i>horizontally loaded</i>

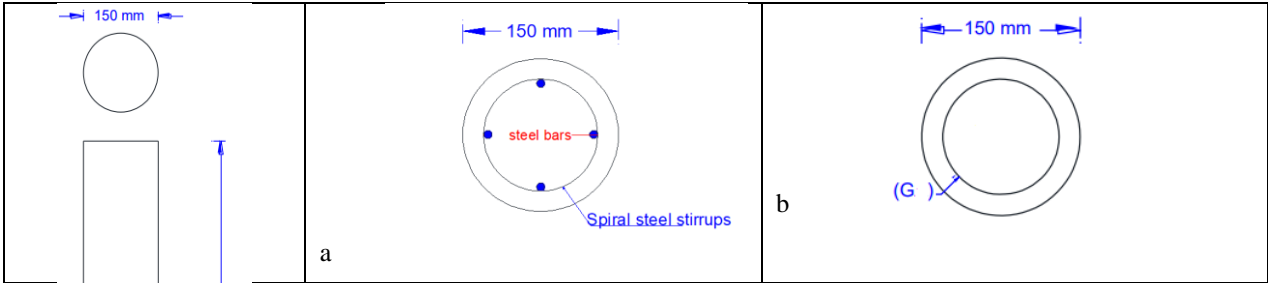
II. EXPERIMENTAL PROGRAM

2.1 Specimens and Test Matrix

five specimens were contained in the experimental program as shown in table 1. The pile specimens were constructed and tested. The tested specimens included five reinforced concrete piles with the same dimensions (150 mm in diameter x 1050 mm in height). The reference pile specimen was reinforced using high tensile steel that formed of four rods with 8 mm diameter and a spiral stirrup of mild steel with 6 mm diameter. The second pile specimen PGH was reinforced using G formed as a cylindrical roll. The other three pile specimens (PSGH, PLGH, and PCGH) were reinforced by cylindrical roll of geogrid with a core of steel, GFRP or CFRP rod in the middle. The horizontally loading test was applied on all specimens. The reinforcing schemes used in the present study according to the previous explanation was shown in figure 1. The variables of the experimental program were the materials used in the reinforcement and the combination of two materials.

Table 1. Test matrix

Group No.	Pile Code	Conditions	Loading Type	Applied Material
Reference	PSH	Reference		Steel Rods (S)
	PGH		Horizontal load	Geogrid (G)
	PSGH			Steel Rod (S) & Geogrid (G)
	PLGH			Glass Fiber Rod (L) & Geogrid (G)
	PCGH			Carbon Fiber Rod (C) & geogrid (G)



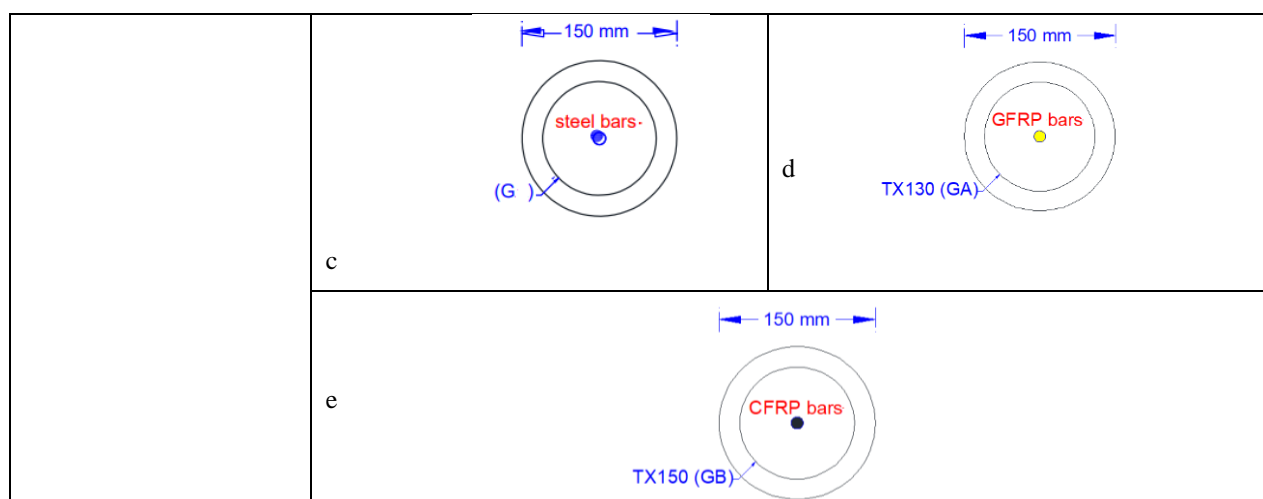


Fig.1 Cross section of composite pile specimens.

(a) Reference pile PSH, (b) PGH, (c) PSG, (d) PLGH, (e)PCGH.

2.2 Material Properties

Ordinary Portland Cement (OPC-42.5 grade), and natural sand with 2.6 fineness moduli with filter stones having a maximum aggregate size of 9 mm were used in the tested specimens. At 28 days, the predicted compressive strength (fcu) was 25 MPa. The actual fcu was gained on the day of testing.

High tensile steel rods grade (40) having 8 mm diameters was used as the main reinforcement of the tested piles. Normal mild steel rods grade (36) was used for spiral stirrups having 6 mm diameter. The reference concrete pile was reinforced with 6 mm diameter normal mild steel as

spiral stirrups and 8 mm diameter high tensile steel rods as vertical reinforcement.

GFRP rods used in this research were manufactured by Russian company Armastek and imported by Fiber Reinforcement Industries Company [22]. According to the manufacturer, the mechanical properties of the GFRP rods were given in Table 2.

Geosynthetics Geogrid manufactured by Tensar International Corporation and imported by National Geotechnical Company for (GEOTECH) [23]. Table 2 gives the mechanical properties of geogrid, according to the manufacturer.

Table 2. Dimensions and characteristic properties of FRP rods. [22],[23]

Features	Geogrid (G)	
Thickness (mm)	1.3	
Tensile strength (N/mm)	10	
Modulus of elasticity (MPa)	200000	
Strain at failure	0.5%	
Features	GFRP rod (L)	
Diameter (mm)	12	
Tensile strength (MPa)	1100	
Modulus of elasticity (MPa)	45000	
Strain at failure	2.2%	
Features	CFRP rod (C)	
Diameter (mm)	12	
Tensile strength (MPa)	1050	
Modulus of elasticity (MPa)	120000	
Strain at failure	0.5%	

2.3 Test Set-Up

The specimens were loaded with a hydraulic jack with a maximum capacity of 1000 (KN), conjoined to electric pump, and suspended with a rigid reaction frame with a maximum capacity of 1000 (KN). The horizontal loaded specimens were placed on two I beam at both sides; one beam represented the pile cap and the other represented the end bearing layer. The load was transferred horizontally by a steel rod to the pile surface using steel plate. The applied loads were measured by a load cell with a maximum capacity of 1000 (KN) located below the hydraulic jack. To monitor displacement for the horizontal loaded specimens, one Linear Variable Differential Transducer (LVDT) was installed beneath the upper third of the pile surface. All test data were collected with a data acquisition

system and collected on a computer at two-second intervals. Figure 2 showed the tests setup which was applied in the concrete laboratory of Benha Faculty of Engineering at the University of Benha.

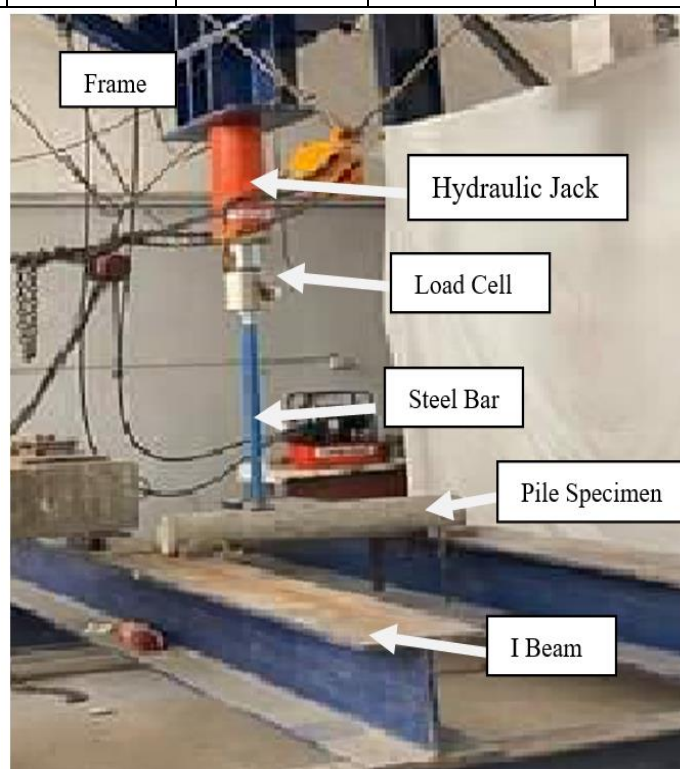
III. EXPERIMENTAL RESULTS AND DISCUSSION

3.1 Ultimate Horizontal Load.

Table 3 presented the ultimate horizontal load (N), deflection at failure (mm), and the cost of reinforcement (L.E.) for tested pile specimens PSH, PGH, PSGH, PLGH, PCGH. The relationship between the horizontal load against the deflection for the experimented pile specimens PSH, PGH, PSGH, PLGH and PCGH was shown in fig. 4.

Table 3. Experimental results

Group No.	Pile Code	Ultimate Horizontal Load (KN)	Ultimate Load/ Ultimate load of PSH %	Deflection at Failure (mm)	Price of Reinforcement (L.E.)	Price of Reinforcement compared to PSH %
Reference	PSH	27.853	Reference Pile	11.30	40	-
	PGH	12.205	44	5.45	6.15	15.25
	PSGH	21.302	76.5	7.35	23.95	59.65
	PLGH	23.655	85	8.7	14.15	35.25
	PCGH	24.21	87	18.5	106.15	265.3



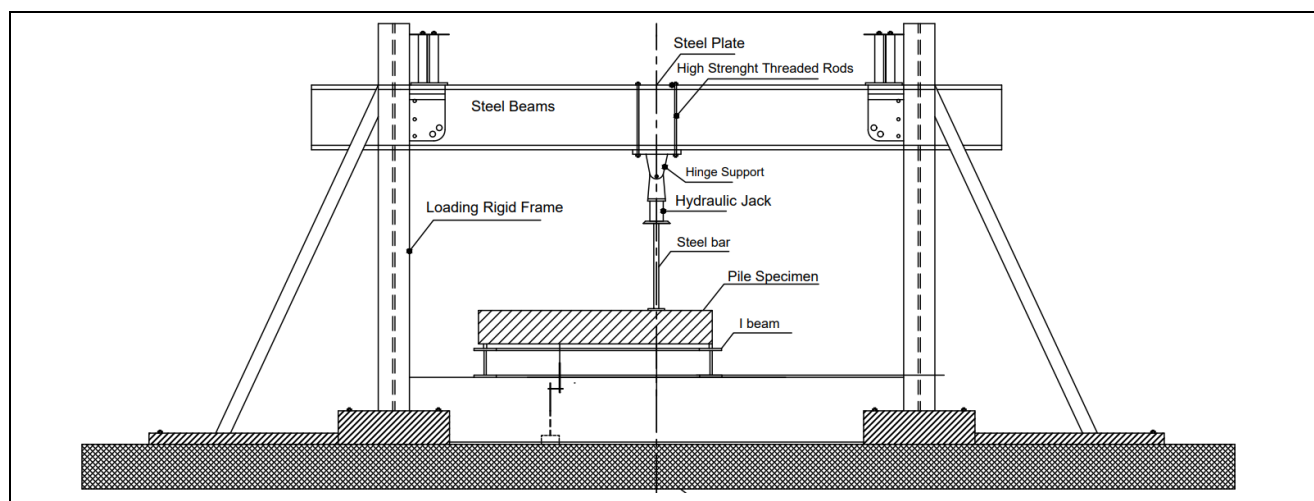


Fig.2 Horizontally loaded test set-up.

3.2 Results and Discussion for Ultimate Horizontal Load

The ultimate horizontal loads for pile specimens PGH, PSGH, PLGH, and PCGH achieved a change of 44%, 76.5%, 85%, and 87% respectively compared to reference pile specimen PSH as shown in Table 3, the use of geogrid resulted a decrease in the ultimate horizontal load, the ultimate horizontal load was decreased to 44% of the reference specimen using geogrids. Also, it was decreased to 76.5% of the reference pile specimen using a core of steel rod with geogrid, while it was decreased to 85% using a core of GFRP rod with geogrid and decreased to 87% using a core of CFRP rod with geogrid. It can be noted that the core of the steel rod or GFRP rod increased the horizontal load with the geogrid.

Comparing the specimens reinforced with different materials and loaded by horizontal load as shown in figure 6, it can be noted that the ultimate horizontal load was

decreased using geogrid with or without a core of (steel, GFRP, CFRP) rod. The reason for this decrement was its ability to make confinement with low tensile strength. It can be noted that using a core of steel rod increased the ultimate horizontal load by 32.5% compared to using geogrid alone, while using a core of GFRP rod increased the ultimate horizontal load by 41% compared to using geogrid alone and using a core of CFRP rod increased the ultimate horizontal load by 43% compared to using geogrid alone. So, using a core of steel rod, GFRP rod or CFRP rod enhanced the horizontal capacity of the pile.

The price of reinforcement for pile specimens PGH, PSGH, PLGH, and PCGH achieved a change of 15.25%, 59.65%, 35.25%, and 265.3% respectively compared to reference pile specimen PSH as shown in Table 3. The price of the reinforcement decreased effectively using the geogrid material alone or with a core of steel or GFRP rod.

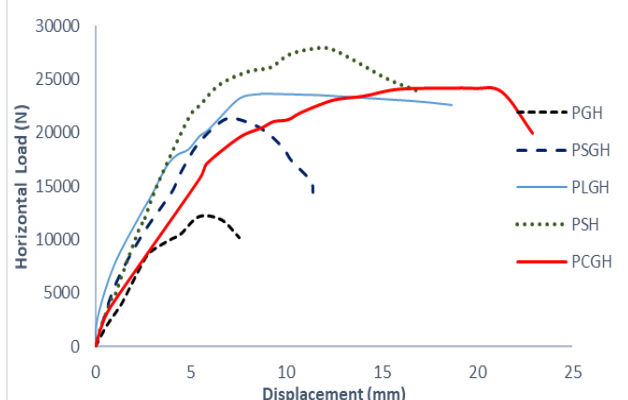


Fig.4 Horizontal load - displacement curve for tested pile specimens PSH, PGH, PSGH, PLGH and PCGH.

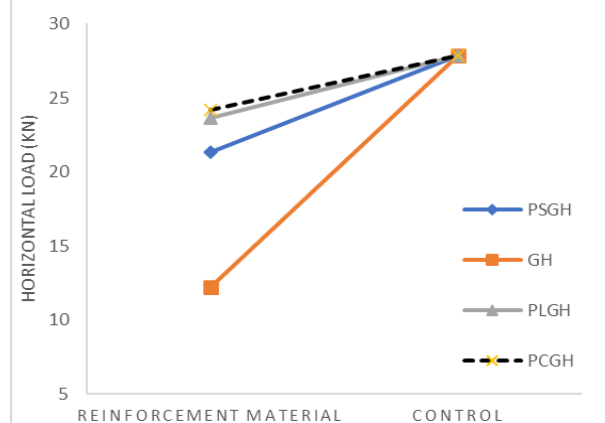


Fig.5 Horizontal load vs reinforcement material relationship for Horizontal loaded specimens

3.3 Modes of Failure

For the reference specimen, the mode of failure acted a ductile failure by tension. For geogrid, or geogrid with a core of steel rod or GFRP rod the modes of failure were a

ductile failure by tension, while for geogrid with a core of steel rod, the mode of failure acted a brittle failure by tension. The modes of failure for all specimens are shown in fig. 6.

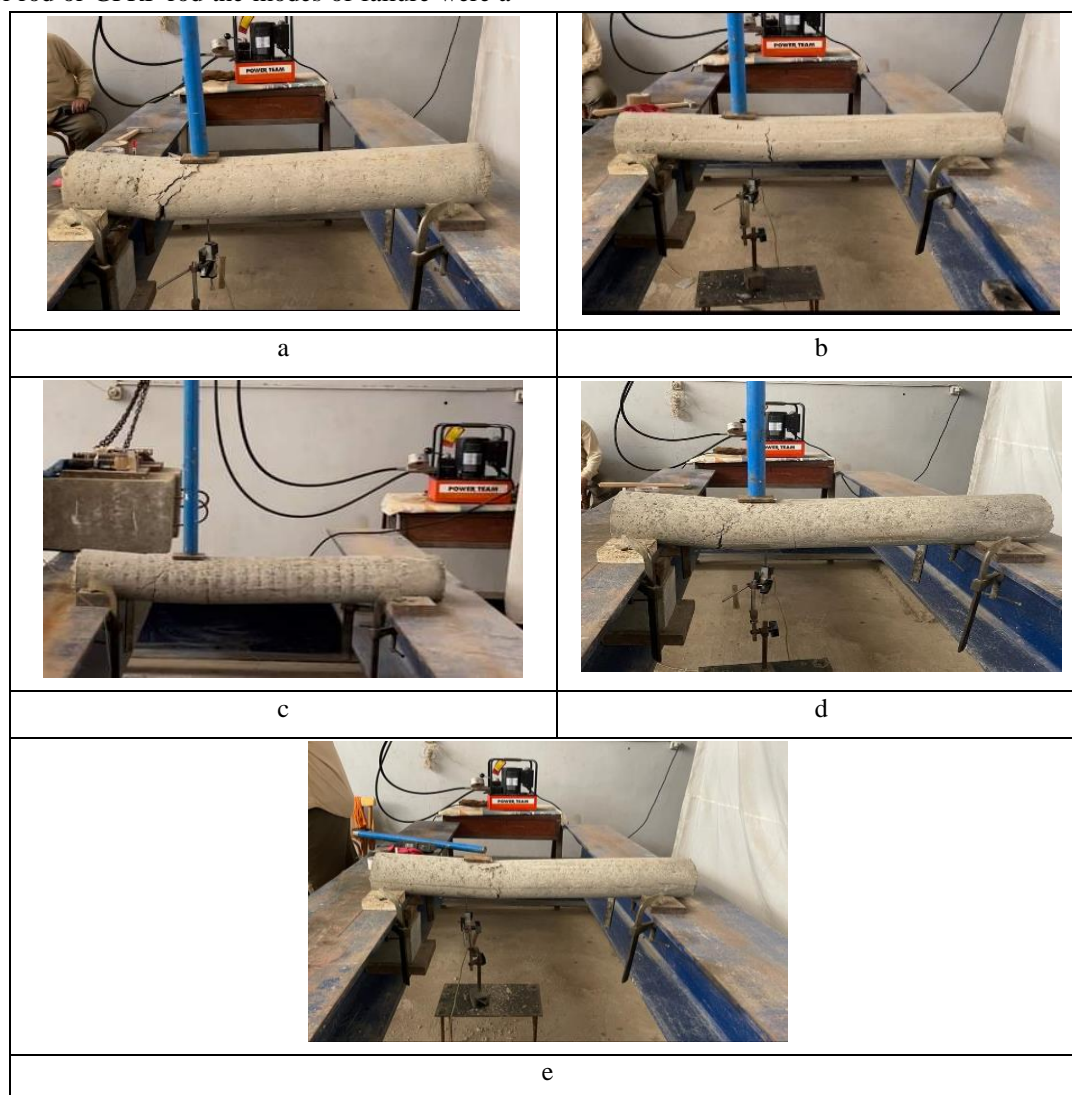


Fig.6 Modes of failure for horizontal loaded specimens

a) PSH b) PGH, c) PSGH, d) PLGH and e) PCGH.

IV. FINITE ELEMENT ANALYSIS

Using a finite-element software Abaqus/CAE standard 6.14-2, a finite-element (F.E) analysis was performed to simulate the behavior of concrete piles reinforced with different materials (steel rods, geogrid and geogrid with steel, CFRP or GFRP rod) under the effect of horizontal load. A lot of features were considered in the F.E.M. as, each part of the model, material properties, the assembly for modeling, the steps of modeling, the contact between the model parts, condition of loading, meshing of the model, and finally solving the model.

The same material properties applied in the experimental program for the concrete, steel, CFRP, GFRP

rods, and geogrids were inputted into the Abaqus software to reproduce the experimental program. The material properties factors were considered in modeling, such as concrete compressive strength, steel, CFRP and GFRP, geogrid tensile strength. A solid part was used to model the concrete. A wire parts were used to model the reinforcement as steel, CFRP or GFRP rods and a shell planar part was used to model the geogrid shell. In the concrete pile, the reinforcement elements were inserted as embedded elements. In the F.E.M, the load was applied horizontally. The modeling of the horizontal loaded pile specimens was shown in figure 7.

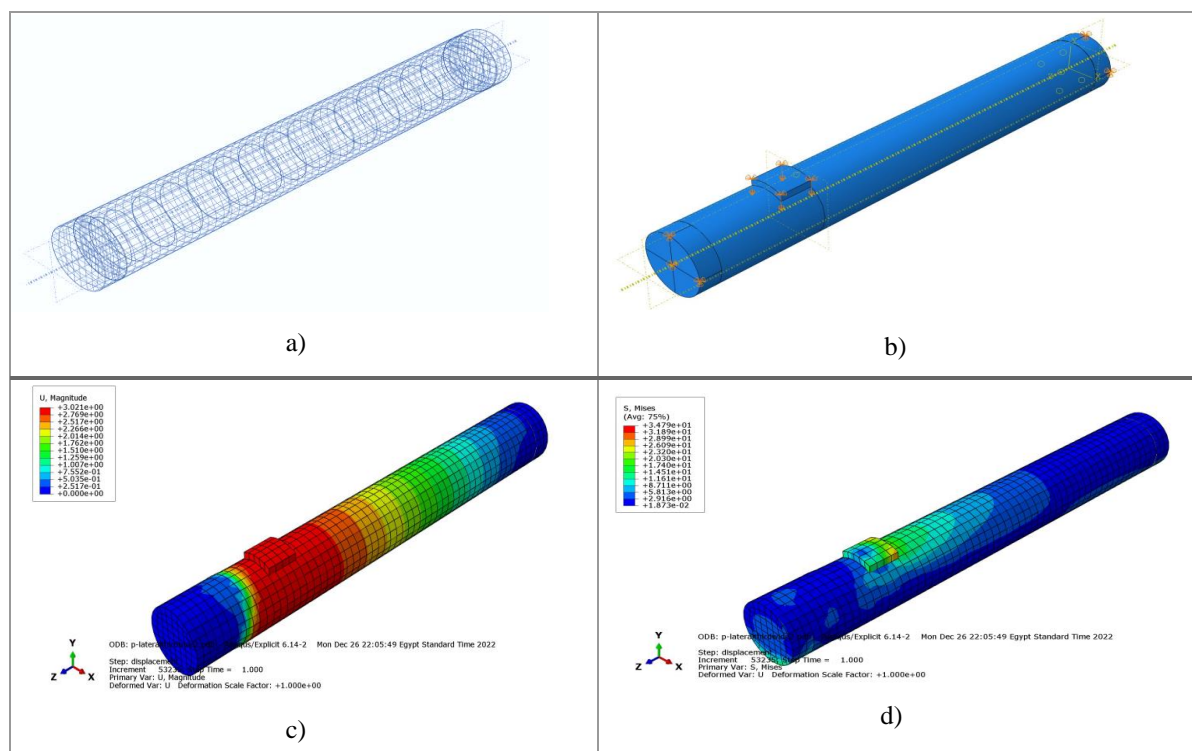
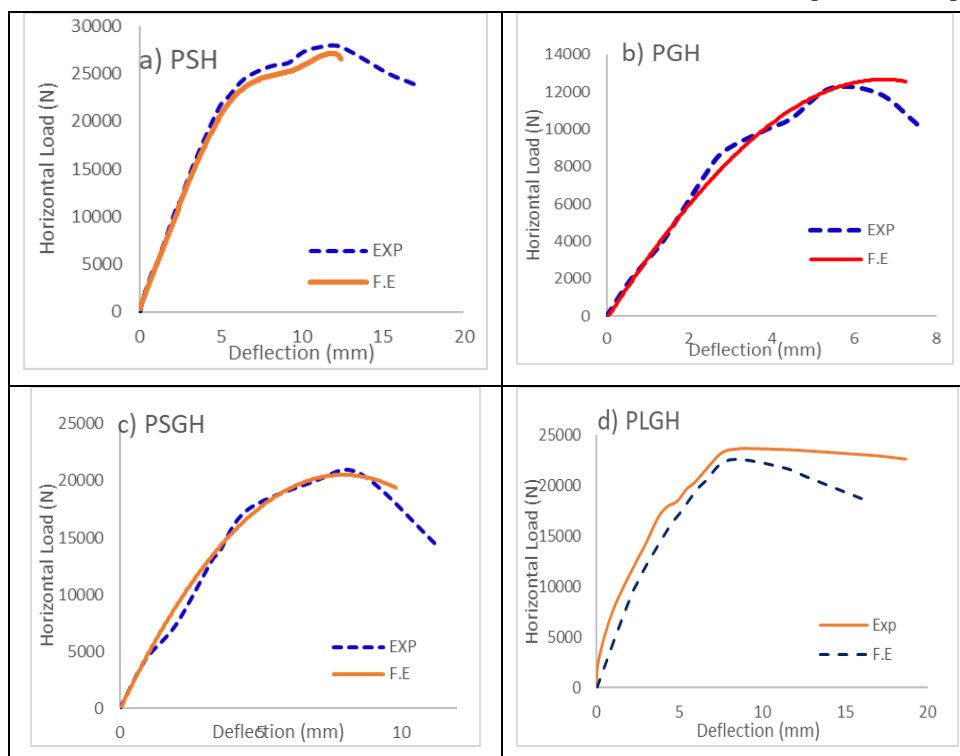


Fig.7 Simulating of horizontal loaded pile specimens.

a) Meshing of the model, b) Loading case, c) The deflection on the model, d) Stresses on the model.

The results gained from the FE modeling were verified with the experimental results. The FE model was used for the verification process of the pile specimens (PSH, PGH, PSGH, PLGH, PCGH). The horizontally loaded specimens PSH, PGH, PSGH, PLGH and PCGH achieved a change in ultimate horizontal load of 107.89%, 99.1%, 101.39%

102.94%, and 101.1% respectively compared to the reference specimen PSH. The experimental, and the FEM ultimate horizontal load results were shown in table (4) and achieved a great convergence as shown. Figure 8 presented the load-deflection curves for the experimental and FEM results of the specimens respectively.



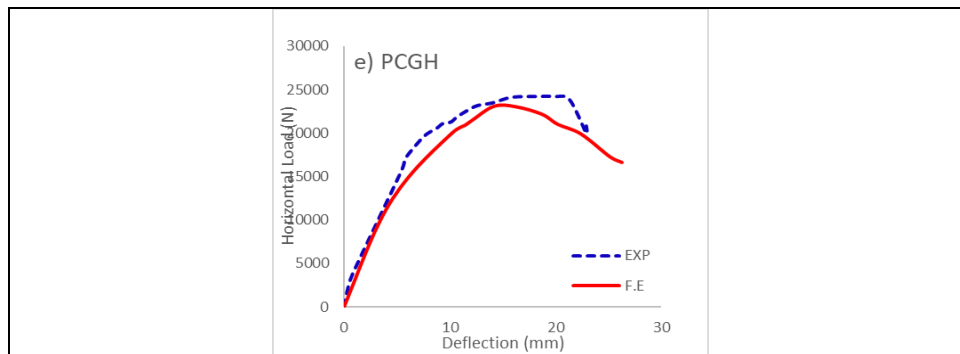


Fig.8 Horizontal load –Displacement relationship for experimental and FEM.

Table 4. Experimental, and FEM results.

Pile Code	V _{EXP} (KN)	V _{FE} . (KN)	V _{EXP} . /V _{FE}
PSH	27.85	25.82	1.08
PGH	12.21	12.31	0.99
PSGH	21.30	21.01	1.01
PLGH	23.66	22.98	1.03
PCGH	24.21	23.95	1.01
	Mean		1.02
	SD		0.0331
	Covariance		0.0011

V. ANALYTICAL CALCULATIONS

All specimens were horizontally loaded. the ultimate predicted horizontal load of the control specimen (pile reinforced with steel rods) can be estimated by applying in equation (1) according to ECP 201 (201) [20] and using interaction diagrams for design circular section under moment.

$$M_u = (K \times e/R) \times R^3 \times f_{cu} \quad (KN.m) \quad (1)$$

Up to now, the ultimate horizontal load of piles reinforcement by geogrids cannot be estimated by ECP 201 (201) [30]. The following paragraph presents suggested equation for specimens reinforced with geogrids which estimated the ultimate horizontal moment by applying in Equation (2). Where, α_s is a reduction factor depends on the position of the reinforcement rod and α_G is a reduction factor depends on the geogrid material. Table (6) presents a comparison between experimental and theoretical results which listed in the same table. A great convergence was verified from the theoretical and experimental results.

$$M_u = (\alpha_G \times (K \times e/R) \times R^3 \times f_{cu}) + (\alpha_s \times (K \times e/R) \times R^3 \times f_{cu}) \quad (KN.m) \quad (2)$$

Where:

- M_u Ultimate horizontal moment on the specimen
- V_u Ultimate horizontal load on the specimen
- f_{cu} concrete compressive strength.
- $K \times e/R$: factor depends on the ratio of reinforcement and the radius of the specimen that can be estimated from the interaction diagram according to ECP 201 (201) [20].
- R : the radius of the specimen.
- α_s : reduction factor depends on the position of the reinforcement rod.
 $\alpha_s = 1$ for steel rods on the edges, $\alpha_s = 0.45$ in the center, $\alpha_s = 0.75$ for FRP rods.
- α_G reduction factor depends on the material.
 $\alpha_G = 0.45$ for the geogrid used.

Table 6: Comparison of Experimental and Theoretical Results.

Pile Code	V _{EXP} (KN)	V _{th.} (KN)	V _{EXP} / V _{th}
PSH	27.853	26.52	1.005
PGH	12.205	11.934	1.095
PSGH	21.302	21.024	0.984
PLGH	23.655	23.25	1.018
PCGH	24.21	23.8	1.01
Mean=			1.022
SD=			0.04299
Covariance =			0.001848

VI. CONCLUSION

- Using geogrid as reinforcement didn't enhance the ultimate horizontal load of the pile.
- The ultimate horizontal load was decreased by 44%- 87% for specimens reinforced by geogrids with or without a core of (steel GFRP or CFRP) rod, but the core of steel, GRFP or CFRP rod was effective in withstanding horizontal load with the geogrid.
- The cost of the reinforcement decreased effectively for the pile specimens reinforced by geogrids and geogrid with a core of steel or GFRP rod, but it increased effectively using a core of CFRP.
- Non-linear finite Element analysis has been verified and achieved a great convergence against the experimental results.
- A theoretical equation has been suggested to predict the ultimate horizontal load which achieved a great convergence with the experimental results.

REFERENCES

- [1] Guades E., Aravinthan T., Islam M., and Manalo A., (2012), "A review on the driving performance of FRP composite piles", Compos Struct, ELSEVIER, Volume 94, Pages 932–1942.
- [2] Giraldo J., and Rayhani M. T., (2014), "Load transfer of hollow Fiber-Reinforced Polymer (FRP) piles in soft clay", Elsevier, Transportation Geotechnics, Volume 1, Pages 63–73.
- [3] Afifi M. Z., Mohamed H. M., and Benmokrane B., (2013), "Axial capacity of circular concrete columns reinforced with GFRP bars and spirals" Journal of Composites for Construction Volume 25.
- [4] Paramanantham N. S., (1993), "Investigation of the behavior of concrete columns reinforced with fiber reinforced plastic rebars", Lamar University.
- [5] Alsayed S. H., Al-Salloum Y. A., Almusallam T. H., and Amjad M. A., (1999), "Concrete columns reinforced by glass fiber reinforced polymer rods", Special Publication. Volume 188, Pages 3-12.
- [6] De Luca A., Matta F., and Nanni A., (2010), "Behavior of full-scale glass fiber-reinforced polymer reinforced concrete columns under axial load", ACI Structural Journal. Volume 107.
- [7] Pantelides C. P., Gibbons M. E., Reaveley L. D., (2013), "Axial load behavior of concrete columns confined with GFRP spirals", Journal of Composites for Construction, Volume 17.
- [8] Mohamed H. M., Afifi M. Z., Benmokrane B., (2014) "Performance evaluation of concrete columns reinforced longitudinally with FRP bars and confined with FRP hoops and spirals under axial load", Journal of Bridge Engineering. Volume 19.
- [9] Tobbi H., Farghaly A. S., and Benmokrane B., (2014), "Behavior of concentrically loaded fiber-reinforced polymer reinforced concrete columns with varying reinforcement types and ratios", ACI Structural Journal Volume 111.
- [10] Hales T. A., Pantelides C. P., and Reaveley L. D., (2016), "Experimental Evaluation of Slender High-Strength Concrete Columns with GFRP and Composite Reinforcement", Journal of Composites for Construction.
- [11] Hadi M. N., and Youssef J., (2016), "Experimental Investigation of GFRP-Reinforced and GFRP-Encased Square Concrete Specimens under Axial and Eccentric Load, and Four-Point Bending Test", Journal of Composites for Construction, Volume 20.
- [12] Karim H., Sheikh M. N., Hadi M. N., (2016), "Axial load-axial deformation behaviour of circular concrete columns reinforced with GFRP bars and helices", Construction and Building Materials, Volume 112.
- [13] Hadi M. N., Karim H., and Sheikh M. N., (2016), "Experimental investigations on circular concrete columns reinforced with GFRP bars and helices under different loading conditions", Journal of Composites for Construction, Volume 9.
- [14] Alajarmeh O., Manalo A., Benmokrane B., Ferdous W., Mohammed A., Abousnina R., Elchalakani M., Edoo A., (2020) "Behavior of circular concrete columns reinforced with hollow composite sections and GFRP bars", Marine Structures, ELSEVIER, Volume 72.
- [15] AlAjarmeh O. S., Manalo A. C., Benmokrane B., Karunasena W., and Mendis P., (2019), "Axial Performance of Hollow Concrete Columns Reinforced with GFRP Composite Bars with Different Reinforcement Ratios," Composite Structures, ELSEVIER, Volume 213, Pages 153-164.

- [16] Guades E. J., Aravinthan T., and Islam M. M., (2011), **“Driveability of composite piles”**, In: Proceedings of the 1st intl postgraduate conference on eddBE2011, Brisbane, Australia, p. 237–42.
- [17] Mirmiran A., and Shahawy Y. S. (2002), **“Analysis and field tests on the performance of composite tubes under pile driving impact”**, Compos Struct, Volume 55.
- [18] Ali A. H., Goudaa A., Mohameda H. M., Rabiea M. H., Benmokraneb B. (2020), **“Nonlinear finite elements modeling and experiments of FRP-reinforced concrete piles under shear loads”**, Structures, ELSEVIER, Volume 28, Pages 106-119.
- [19] Pando A. M., Ealy C. D., Flitz M. G., Lesko J. J., and Hoppe E. J., (2006), **“A laboratory and field study of composite piles for bridge substructures”**, McLean, VA: Federal Highway Administration, Report No. FHWA-HRT04-043.
- [20] ECP-Egyptian Code of Practice-201. (2011), **“Egyptian code of Practice”**, No. 201 for calculating loads and forces in structural work and masonry, National Research Center for Housing and Building, Ministry of Housing, Utilities and Urban Planning, Cairo.