[1] **Dr.Daniel Madan Raja S**

[2] **Ms.Vipparthi Susanna***

[3] **Dr.Srinitya G**

[4] **Dr.Ramesh C**

[5] **Dr.Thomas Samraj Lawrence**

[6] **Mr. Ganapathy Dharmalingam**

Leveraging Digital Forensics in the Age of Smart Grids: A Survey of Tools and Techniques for Securing Electrical Power Systems

Journal of Electrical Systems

Abstract: - The increasing reliance on digital technologies in smart grids introduces vulnerabilities to cyberattacks that can disrupt critical infrastructure and impact daily life. For critical infrastructures to be protected against potential cyber-attacks, many forensic approaches have already been developed to collect, analyze, and digitalize the evidence to assist in the in-depth investigation of any incident. The growing complexity of power grids with interconnected digital components necessitates robust security measures. The modern power grids are not isolated they are interconnected networks of controls where if one component or system is affected the whole system faces a blackout. Network forensics plays a crucial role in investigating these attacks, identifying the source, and implementing mitigation strategies. This paper compares and analyzes three key tools: Wireshark, Nmap and NetMiner used in the network forensics of electrical power systems focusing on their performance assessed against various parameters.

Keywords: Smart Grid, Electrical Power System, Cyberattack, Network Forensics, Wireshark, Nmap, NetMiner

I. INTRODUCTION

The electrical power system is a complex network that generates, transmits, and distributes electricity to various locations. It involves several stages, starting from the generation of electricity to its consumption. Electrical power generation is the first stage in the electrical power system. Different types of power plants utilize various methods to convert other forms of energy into electrical energy. Some common methods include Thermal Power Plants: These plants burn fossil fuels (coal, natural gas) to heat water, creating steam that drives turbines, generating electricity. Hydropower Plants: These plants utilize the energy of moving water (rivers, dams) to spin turbines and generate electricity. Wind Power Plants: These plants convert wind energy into electricity using wind turbines. Solar Power Plants: These plants convert sunlight into electricity using photovoltaic cells (solar panels). Nuclear Power Plants: These plants use nuclear fission to produce heat, which then creates steam to drive turbines and generate electricity. Generating Stations are where electric power is produced by parallel-connected three-phase alternators or generators. The power plant's capacity and generating voltage vary but are often stepped-up using transformers for efficient transmission. Various types include thermal, hydropower, nuclear, diesel, gas, solar, tidal, and wind power plants, each serving different purposes based on their characteristics and locations.

Electricity generated at power plants needs to be transported over long distances to reach consumers. This is where transmission lines come into play. These are high-voltage lines (often exceeding 100,000 volts) strung across tall

[1] Associate Professor, Division of CSE, School of CST, Karunya Institute of Technology and Sciences, Coimbatore-641114.

[2] *Corresponding Author: PG Student, Division of CSE, School of CST, Karunya Institute of Technology and Sciences, Coimbatore-641114.

[3] Associate Professor, Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering, Coimbatore-641202.

[4] Associate Professor, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore – 632014.

[5] Associate Professor, Department of IT, College of Engineering and Technology, Dambi Dollo University, Ethiopia – 260.

[6] Deputy General Manager, Adani Renewable Energy Ltd., Shantigram, Ahmedabad, Gujarat, 382421.

[1]danielmadanraja@karunya.edu, [2]vipparthisusanna@karunya.edu.in, [3]srinitya.g@sece.ac.in, [4] rameshc70707@gmail.com, [5]samraj@dadu.edu.et , [6]ganapathy.dharmalingam@adani.com

towers, minimizing energy loss during transmission. Substations play a crucial role in the transmission system. They step up the voltage generated at power plants to significantly higher levels for efficient long-distance transmission. They also step down the voltage at various points in the grid to levels suitable for local distribution networks. They act as interconnection points where different power plants and transmission lines connect as well.

After electricity is transmitted through high-voltage lines and reaches substations, the distribution stage of the electrical power system takes over to deliver power to individual consumers efficiently. This crucial phase involves the distribution network, which comprises various components to ensure electricity reaches homes and businesses seamlessly. There are three main components involved in the distribution. Substation Transformers: These transformers play a vital role in the distribution network by further reducing voltage levels to suitable ranges for homes and businesses. Typically, voltages are adjusted to around 120 or 240 volts for safe consumption by end-users. Distribution Lines: Unlike high-voltage transmission lines, distribution lines are lower-voltage lines that branch out from substations and extend into neighbourhoods or individual buildings. These lines form the final link in the chain, delivering electricity directly to consumers. Distribution Transformers: At the final stage of distribution, distribution transformers lower the voltage even further to meet the specific voltage requirements of appliances and equipment used by consumers. This step ensures that electricity is delivered at appropriate voltages for various devices in homes and businesses.

Cyber-attacks have increased by 38% globally by 2022, with an increase of 48% for the utilities of smart energy [2]. The U.S. energy infrastructure has also been proactive against the alarming threats to the US Energy Grid since the cyber-attacks have increased to 22% by 2022 [28]. This paper studies the comparison of the application of Wireshark, Nmap and NetMiner for the identification and after-attack procedures to perform network forensics faced by the Electrical Smart Grid.

II. LITERATURE REVIEW

Electrical network forensics attracts diverse interests that have ultimately led to the publication of their research works in this regard to bridge the gap within the domain.

Research has been carried out for the protection of Power Systems. In [2], proactive digital forensic modelling approaches have been proposed that focus on Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICSs) and automation. The authors in [9], implemented cyber-attacks on a power grid substation set up in the lab, with intelligent Electronic Devices to investigate the attacks which exploited IEC 61850 and GOOSE protocols. In [15], OSCAR methodology, logging architecture and the methodological framework were proposed for crime investigation in smart grid networks. In [20], the authors proposed cybersecurity protection for power grid control systems. In [22], the authors performed an anatomy of an electrical substation failure in a Brazilian Chemical Plant and analyzed its forensics. In [23], the authors performed anti-forensics on an electrical network to analyze its network frequency and proposed countermeasures for the same. In [24], the electrical power system monitoring was performed using the Dynamic System Monitoring (DSM) method and analyzed the outcomes. The authors in [25], assessed a power plant to know the severity of its vulnerability. In [26], a case study was carried out on the damage of a distribution transformer due to through-fault currents.

Research has been carried out on the various network forensic tools that can be used in terms of their functionality to analyze network-based attacks. In [10], the authors surveyed the state-of-the-art tools for computer forensics. The survey toolkits included Autopsy, RDLine, Belkasoft, OS, ProDiscover, XWays, EnCase and FTK. In [1], the authors compared the performance of forensics tools and tested the scenarios based on NIST SP 800-101 R1. The accuracy of the digital evidence obtained by the UltData Android tool was 95%, Wondershare Dr.Fone was 50% and the EaseUs mobisaver tool was 20%. In [3], the authors documented how a toolkit based on Nmap helps beginners to achieve the same results easily. In [4], a case study was documented on the network vulnerability assessment of 50 Indian Government e-portals with the deployment of the Nmap tool. In [5], the authors proposed an automated log analysis that requires only sensitive data such as the network's current status and messages related to that status. 30 days of logs were collected using the PRTG network monitoring tool, and the data was analyzed using the mining technique Fpmax. This was efficient in identifying patterns in logs generated by network monitoring software which leveraged NetMiner. In [6], a case study was documented on the network security assessment of 50 Indian Company portals using Nmap for examining the networks. In [7], the authors proposed an automated tool using machine learning algorithms to combine different vulnerability data sources to minimize the time and effort of forensic procedures in critical energy infrastructures. In [8], the authors presented 3 instruments for the development of sound machine-driven digital forensics methodologies for evaluation, standardization and optimization which apply to the AI models. In [18], the authors compared and analyzed various network forensic tools on different operating systems. The analysis included the tools Wireshark, Ettercap, Etherape, Kismet, Network Miner, TcpDump, WinDump, Cloud Shark, Colasoft Capsa, Sysdig, Debokee, Etheral, Intercepter NG, Nethogs, MNM, SmartSniff, PacketSled, Scapy, Cain and Abel, Savvius Omnipeek, Packet Peeker, CPA, KisMac. In [12], the authors reviewed the OSCAR methodology and the tools and techniques for network forensics. The tools included were Wireshark, Tshark, Dumpcap, and NFATs. In [13], the authors studied a few open-source forensic tools and performed a comparative analysis based on 6 key parameters. Wireshark, Nmap, Nessus, Snort, and Ettercap tools were used for the purpose. In [14], the authors surveyed the main issues involved in the complex process of IoT-based investigations including the overview of past and current theoretical models in digital forensics. In [17], the researchers developed a stress testing platform specifically tailored to assess the robustness and reliability of digital forensic tools using the Sleuth Kit framework. In [18], the authors proposed a method to timely detect the adversarial attack on the power grid and assessed the state based on data from the PMUs collected and processed in the PDC. The authentication attack scenario was successfully executed on the power station setup. In [19], the authors surveyed the literature on digital forensics for SCADA, proposed frameworks, and methodologies. In [21], two electrical power system failure cases have been studied and documented. In [16], the authors proposed D4I, a digital forensics framework including digital artefacts categorization and mapping to the cyber kill chain steps, steps for examination and analysis phases including an application use case of a spear-phishing attack.

Although the research work carried out over the years in this domain included the network forensic analysis of the electrical power systems it did not involve the use of various forensic tools like Nmap, Wireshark and NetMiner. Hence, the application of these tools for that purpose was studied and their performance metrics were analysed.

III. METHODS

The Smart Grid Technology

Smart grid technology as shown in Fig. 2., represents a significant leap in the evolution of the traditional power grid, ushering in a new era of digital transformation and efficiency. This innovative approach incorporates advanced technologies to enhance the functionality and responsiveness of the electrical grid, offering numerous benefits to both utilities and consumers. The Smart Grid is a modernized electrical grid that integrates advanced technologies for efficient energy management and is vulnerable to various cyber-attacks that can disrupt operations and compromise data integrity. Understanding the networks within the smart grid and potential attacks necessitating network forensics is crucial for safeguarding critical infrastructure. Key components in the Smart Grid are- Smart Meters: These intelligent devices enable real-time tracking of electricity consumption, fostering two-way communication between consumers and utilities. Smart meters play a crucial role in providing accurate data on energy usage, enabling better management and optimization of electricity distribution. Sensors: Integrated sensors collect essential data points such as voltage fluctuations, equipment health, and environmental conditions. This data provides valuable insights into grid operations, allowing for proactive maintenance and improved decision-making processes. Advanced Control Systems: Utilizing the data collected by sensors and smart meters, advanced control systems optimize power generation, distribution, and consumption within the grid. By leveraging automation and data analytics, these systems aim to enhance efficiency, reliability, and responsiveness across the entire grid infrastructure.

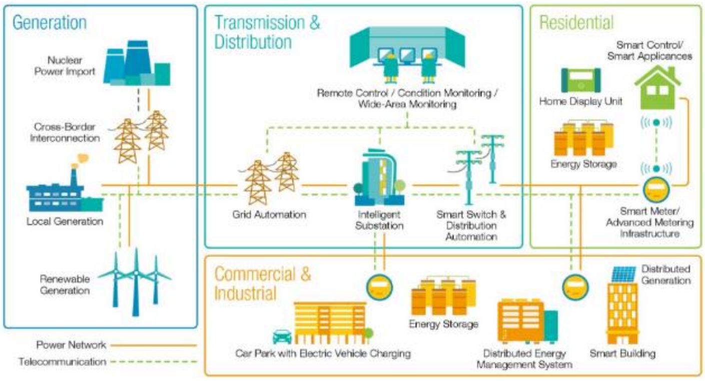

Generation
Nuclear Power Import
Cross-Border Interconnection
Local Generation
Renewable Generation
Power Network
Telecommunication
Transmission & Distribution
Remote Control / Condition Monitoring / Wide-Area Monitoring
Grid Automation
Intelligent Substation
Smart Switch & Distribution Automation
Residential
Smart Control/ Smart Applicances
Home Display Unit
Energy Storage
Smart Meter/ Advanced Metering Infrastructure
Commercial & Industrial
Energy Storage
Distributed Generation
Car Park with Electric Vehicle Charging
Distributed Energy Management System
Smart Building

Figure 1. The Smart Grid [30]

Firstly, the Communication Networks. These networks facilitate data exchange between different components of the smart grid, enabling real-time monitoring and control. Secondly, the Control Systems manage the operation of devices within the grid, ensuring optimal performance and reliability. Thirdly, Information Technology (IT) Networks support administrative functions and data management within the smart grid infrastructure.

A. Networks in the Smart Grid

Firstly, the Communication Networks. These networks facilitate data exchange between different components of the smart grid, enabling real-time monitoring and control. Secondly, the Control Systems manage the operation of devices within the grid, ensuring optimal performance and reliability. Thirdly, Information Technology (IT) Networks support administrative functions and data management within the smart grid infrastructure.

B. Areas vulnerable to potential Cyber-attacks in the Smart Grid

SCADA Systems

Attacks: Cybercriminals may manipulate control signals, make unauthorized configuration changes, or introduce targeted malware to disrupt power generation, substation control, or trigger outages. Network Forensics: Analysis of SCADA system logs, network traffic, and control commands is essential to identify anomalies, unauthorized access, and malicious activities within SCADA systems.

Substations

Attacks: Substation control systems can be disrupted, leading to power outages or physical equipment damage. Network Forensics: Examination of network traffic within substations helps in detecting suspicious communications, unauthorized access attempts, and potential firmware tampering.

Transmission Lines

Attacks: Monitoring and control systems for transmission lines are vulnerable to attacks that can compromise operational stability and visibility. Network Forensics: Analysis of sensor data, control system logs, and communication traffic aids in identifying unauthorized activities and potential sabotage attempts.

Smart Meters

Attacks: Smart meters are at risk of firmware manipulation, data theft, or being recruited into botnets for large-scale attacks. Network Forensics: Scrutinizing smart meter communication logs is crucial to detect malicious activities like firmware tampering and unauthorized data access attempts.

Communication Networks

Attacks: Disruption of communication networks can impact real-time monitoring, control, and automated responses, potentially leading to grid instability and cascading failures. Network Forensics: Examination of network traffic helps pinpoint Denial-of-Service (DoS) attacks, intrusion attempts, and potential malware propagation within communication networks.

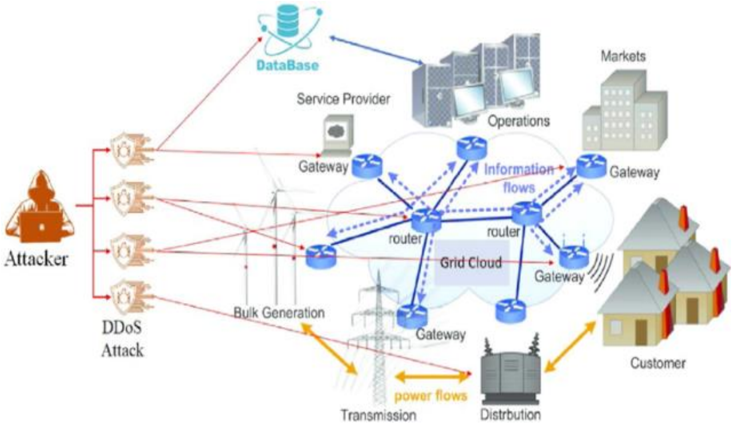


Figure 3. Potential Cyberattack Paths in the Smart Grid Network [31]

C. The Network Forensics Process Flow

The network forensics process flow after an attack involves several key steps:
Identification: Recognizing and determining an incident based on network indicators is crucial to kickstart the investigation.

- Preservation: Isolating and securing data to prevent tampering is essential for maintaining the integrity of evidence.

- Collection: Recording the physical scene and duplicating digital evidence using standardized methods is necessary for further analysis.

- Examination: Keeping a record of all visible data, including metadata, which can be crucial for court proceedings.

- Analysis: Reconstructing data fragments and drawing conclusions based on the evidence gathered, often aided by tools like Security Information and Event Management (SIEM) software.

- Presentation: Summarizing and explaining conclusions in layperson's terms using abstracted terminologies for clarity.

- Incident Response: Validating and assessing the intrusion detected based on the gathered information to take appropriate actions.

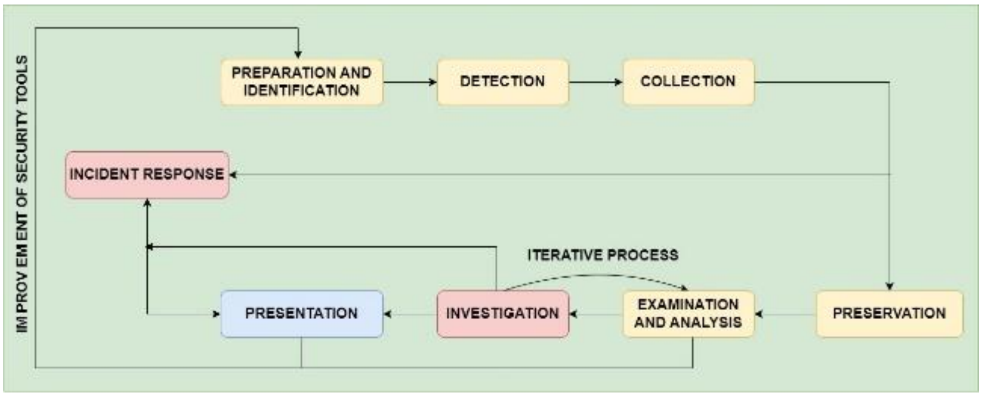


Figure 4. Network Forensics Process Flow

D. Leveraging wireshark, nmap and network miner (netminer) for smart grid forensics

Wireshark

Wireshark is an open-source network packet analyzer that supports real-time data interception and decryption. It is widely used for network forensics due to its extensive protocol support, live capture, and offline analysis capabilities. Key features include Extensive protocol support: Wireshark can analyze hundreds of protocols, including VoIP, IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2. Live capture and offline analysis: Wireshark can capture network traffic in real time and analyze it later for forensic purposes. Color-coded packet list: Packets can be colored based on rules for quick analysis. VoIP analysis: Wireshark supports detailed VoIP analysis, which is crucial for smart grid security.

When conducting network forensics on a smart grid after a fault has occurred, Wireshark can be a valuable tool for in-depth analysis. We have given a detailed use of Wireshark in the context of a smart grid post-fault.

• Packet Capture: Start Wireshark and select the network interface capturing packets from the smart grid system, such as Ethernet or Wi-Fi.

• Analysis Windows: Wireshark will capture packets in real time and display them in three separate analysis windows:

Packet List Pane: Shows color-coded packets moving in real-time.
Packet Details Pane: Provides header information from selected packets.

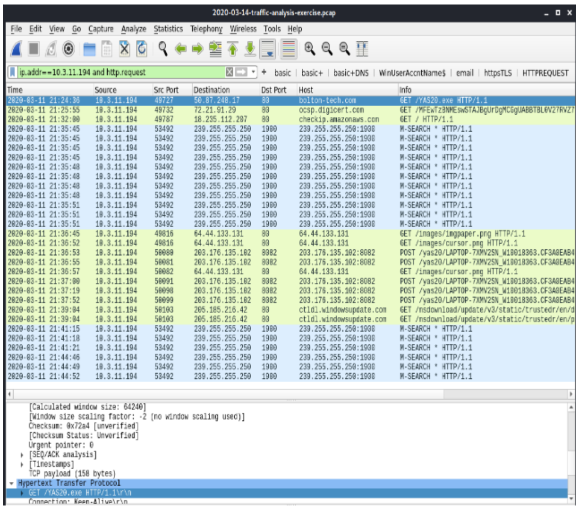
Packet Bytes Pane: Displays payload information in hexadecimal and ASCII formats.

• Creating Filters: To manage the overwhelming amount of data, use Wireshark's filtering language to focus on specific packets of interest for forensic analysis.

• Follow Stream: Follow a stream of communication to track conversations or activities within the smart grid system. Right-click on a packet, select "Follow," then "TCP Stream" to view all packets in that stream.

• Statistics: Utilize Wireshark's statistics feature to gather insights and create baselines of normal traffic within the smart grid system. Navigate to IPv4 Statistics and All Addresses to view detailed statistics for each IP address captured.

• Security Measures: Ensure proper security practices when using Wireshark, such as not running it as an admin/root user and shutting it down after use to reduce security risks.



ip.addr==10.3.11.194 and http.request

Time	Source	Src Port	Destination	Dst Port	Host	Info
2020-03-11 21:24:36	10.3.11.194	49727	50.87.248.17	80	bolton-tech.com	GET /YAS20.exe HTTP/1.1
2020-03-11 21:25:55	10.3.11.194	49732	72.21.91.29	80	ocsp.digicert.com	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7
2020-03-11 21:32:00	10.3.11.194	49787	18.235.112.207	80	checkip.amazonaws.com	GET / HTTP/1.1
2020-03-11 21:35:45	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:45	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:45	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:45	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:48	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:48	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:48	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:48	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:51	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:51	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:35:51	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:36:45	10.3.11.194	49816	64.44.133.131	80	64.44.133.131	GET /images/imgpaper.png HTTP/1.1
2020-03-11 21:36:52	10.3.11.194	49816	64.44.133.131	80	64.44.133.131	GET /images/cursor.png HTTP/1.1
2020-03-11 21:36:53	10.3.11.194	50080	203.176.135.102	8082	203.176.135.102:8082	POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB4
2020-03-11 21:36:55	10.3.11.194	50081	203.176.135.102	8082	203.176.135.102:8082	POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB4
2020-03-11 21:36:57	10.3.11.194	50082	64.44.133.131	80	64.44.133.131	GET /images/cursor.png HTTP/1.1
2020-03-11 21:37:00	10.3.11.194	50091	203.176.135.102	8082	203.176.135.102:8082	POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB4
2020-03-11 21:37:19	10.3.11.194	50098	203.176.135.102	8082	203.176.135.102:8082	POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB4
2020-03-11 21:37:52	10.3.11.194	50099	203.176.135.102	8082	203.176.135.102:8082	POST /yas20/LAPTOP-7XMV2SN_W10018363.CF3A0EAB4
2020-03-11 21:39:04	10.3.11.194	50103	205.185.216.42	80	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en/d
2020-03-11 21:39:04	10.3.11.194	50103	205.185.216.42	80	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en/p
2020-03-11 21:41:15	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:41:18	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:41:21	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:44:46	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:44:49	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2020-03-11 21:44:52	10.3.11.194	53492	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1

```
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x72a4 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (158 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /YAS20.exe HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
```

Figure 5. Working of Wireshark

Nmap

Nmap (Network Mapper) is a network scanning and auditing tool that can be used for network forensics. It is known for its ability to discover hosts and services on a network, which can be useful for incident response and forensic analysis. Key features include Network discovery: Nmap can scan a network to identify hosts and services, providing valuable information for forensic analysis. Port scanning: It can scan ports on a network to identify open ports and services, which can help in understanding network vulnerabilities. OS detection: Nmap can determine the operating system of a target host, which can be useful for forensic analysis.

After a fault occurs in the smart grid, utilizing Nmap for network forensics can provide valuable insights into the network's security posture and aid in identifying vulnerabilities or malicious activities. We have given a detailed use of Nmap in the context of a smart grid post-fault.

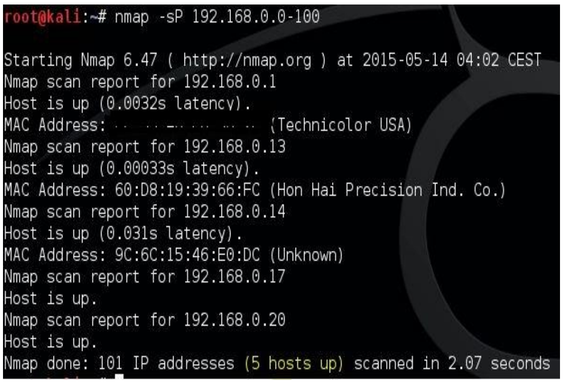
• Network Discovery: Identify all hosts and devices connected to the smart grid network.
Nmap Command: Utilize Nmap's network scanning capabilities to discover active hosts, open ports, and services running on each device. nmap -sn <target_IP_range> to perform a ping scan to identify live hosts.
• Port Scanning: Identify open ports on critical devices within the smart grid network. Nmap Command: Conduct port scanning to determine which services are running on specific ports. nmap -p- <target_IP> to scan all ports on a specific host.

• Service Version Detection: Determine the versions of services running on open ports for potential vulnerabilities. Nmap Command: Use service version detection to gather information about running services. nmap -sV <target_IP> to detect service versions on open ports.

• Operating System Detection: Identify the operating systems of devices connected to the smart grid network. Nmap Command: Employ OS detection capabilities to determine the OS running on each host. nmap -O <target_IP> to detect the operating system of a target host.

• Scripting Engine: Automate tasks and perform customized scans for specific forensic requirements. Nmap Scripting Engine (NSE): Create custom scripts or use existing scripts to gather detailed information about network devices. nmap --script=<script_name> <target_IP> to run a specific NSE script.

• Output Analysis: Analyze Nmap scan results to identify anomalies, unauthorized services, or potential security weaknesses. Nmap Output Formats: Review Nmap output in various formats like XML, grepable, or interactive mode for detailed analysis.



```
root@kali:~# nmap -sP 192.168.0.0-100

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-14 04:02 CEST
Nmap scan report for 192.168.0.1
Host is up (0.0032s latency).
MAC Address: [redacted] (Technicolor USA)
Nmap scan report for 192.168.0.13
Host is up (0.00033s latency).
MAC Address: 60:D8:19:39:66:FC (Hon Hai Precision Ind. Co.)
Nmap scan report for 192.168.0.14
Host is up (0.031s latency).
MAC Address: 9C:6C:15:46:E0:DC (Unknown)
Nmap scan report for 192.168.0.17
Host is up.
Nmap scan report for 192.168.0.20
Host is up.
Nmap done: 101 IP addresses (5 hosts up) scanned in 2.07 seconds
```

Figure 6. Working of Nmap

Network Miner (NetMiner)

NetMiner is an open-source network forensic analysis tool (NFAT) that works on Windows, Linux, Mac OS X, and FreeBSD. It can be used as a passive network sniffer/packet-capturing tool to detect operating systems, sessions, and other network activities. Key features include a Passive network sniffer: NetMiner can capture network traffic without interfering with the network. Packet decoding: It can decode various network protocols, including TCP/IP, UDP, ICMP, and others. Session identification: NetMiner can identify and track network sessions for forensic analysis.

NetMiner can be effectively utilized in the context of a smart grid post-fault scenario to conduct network forensics. We have given a detailed use of NetMiner in the context of a smart grid post-fault.

• Identification of Fault: After a fault occurs in the smart grid, the first step is to identify the nature and extent of the fault, whether it's a cyber-attack, system malfunction, or other issues affecting the grid's operations.

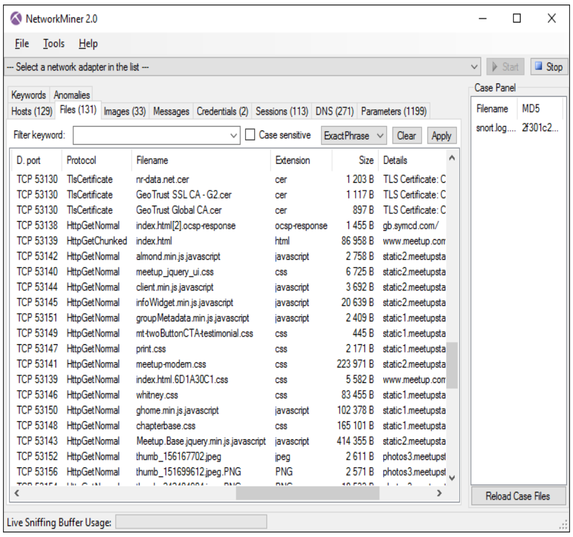
• Launching NetMiner: Start by launching NetMiner on the system where network traffic needs to be analyzed. NetMiner can work on various operating systems like Windows, Linux, Mac OS X, and FreeBSD.

• Data Capture: NetMiner operates as a passive network sniffer and packet-capturing tool. Begin capturing network traffic to analyze the data packets flowing through the network post-fault.
• Packet Decoding: Utilize NetMiner's packet decoding capabilities to extract information from captured packets related to communication protocols, data exchanges, and potential anomalies that might have caused the fault.

• Session Identification: NetMiner can identify and track network sessions, helping in reconstructing the sequence of events leading up to the fault within the smart grid infrastructure.

• Anomaly Detection: Analyze the captured network traffic using NetMiner to detect any unusual patterns, unauthorized access attempts, or malicious activities that could have triggered the fault in the smart grid.

• Forensic Analysis: Conduct a thorough forensic analysis using NetMiner's features to delve deeper into the network data, identify potential security breaches or vulnerabilities, and gather evidence for further investigation or remediation.



Filter keyword: □ Case sensitive ExactPhrase Clear Apply

D. port	Protocol	Filename	Extension	Size	Details
TCP 53130	TlsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C
TCP 53138	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb.symcd.com/
TCP 53139	HttpGetChunked	index.html	html	86 958 B	www.meetup.com
TCP 53142	HttpGetNormal	almond.min.js.javascript	javascript	2 758 B	static2.meetupsta
TCP 53140	HttpGetNormal	meetup_jquery_ui.css	css	6 725 B	static2.meetupsta
TCP 53144	HttpGetNormal	client.min.js.javascript	javascript	3 692 B	static2.meetupsta
TCP 53145	HttpGetNormal	infoWidget.min.js.javascript	javascript	20 639 B	static2.meetupsta
TCP 53151	HttpGetNormal	groupMetadata.min.js.javascript	javascript	2 409 B	static1.meetupsta
TCP 53149	HttpGetNormal	mt-twoButtonCTA-testimonial.css	css	445 B	static1.meetupsta
TCP 53147	HttpGetNormal	print.css	css	2 171 B	static1.meetupsta
TCP 53141	HttpGetNormal	meetup-modern.css	css	223 971 B	static2.meetupsta
TCP 53139	HttpGetNormal	index.html.6D1A30C1.css	css	5 582 B	www.meetup.com
TCP 53146	HttpGetNormal	whitney.css	css	83 455 B	static1.meetupsta
TCP 53150	HttpGetNormal	ghome.min.js.javascript	javascript	102 378 B	static1.meetupsta
TCP 53148	HttpGetNormal	chapterbase.css	css	165 101 B	static1.meetupsta
TCP 53143	HttpGetNormal	Meetup.Base.jquery.min.js.javascript	javascript	414 355 B	static2.meetupsta
TCP 53152	HttpGetNormal	thumb_156167702.jpeg	jpeg	2 611 B	photos3.meetupst
TCP 53156	HttpGetNormal	thumb_151699612.jpeg.PNG	PNG	2 571 B	photos3.meetupst

Filename	MD5
snort.log....	2f301c2...

Figure 7. Working of NetMiner

E. Comparative Analysis

When evaluating the ease of use of Wireshark, NetMiner, and Nmap for network forensics post-fault analysis in smart grids, the following insights can be derived:

Wireshark:

• User-Friendly Interface: Wireshark offers a user-friendly interface with features like live packet capture and detailed network traffic analysis.

- Ease of Navigation: It provides a straightforward process for capturing and analyzing network packets, making it accessible for users with varying levels of expertise.

- Extensive Protocol Support: Wireshark's support for numerous protocols and real-time data decryption enhances its usability for network forensics tasks.

NetMiner:

- Automatic File Extraction: NetMiner is praised for its automatic extraction of files from packet captures, simplifying the process for users.

- Message Extraction: It excels in extracting messages like emails, enhancing usability for specific forensic tasks.
- Limited Manual Packet Analysis: While NetMiner may lack in manual packet analysis compared to Wireshark, its focus on automated extraction makes it user-friendly for certain tasks.

Nmap:

- Network Scanning Utility: Nmap's network scanning and auditing capabilities provide a straightforward approach to mapping network services and vulnerabilities.

- User-Friendly Features: With functions like port scanning and service discovery, Nmap offers an intuitive interface for users to conduct network reconnaissance.

- Internal Network Auditing: It allows internal network auditing, making it user-friendly for network administrators to monitor host and service uptime.

In summary, Wireshark stands out for its user-friendly interface, extensive protocol support, real-time analysis capabilities, and accuracy NetMiner offers ease of use through automatic file extraction but may lack in manual packet analysis compared to Wireshark. Nmap provides a straightforward approach to network scanning and auditing tasks, making it suitable for mapping network vulnerabilities and services with ease.

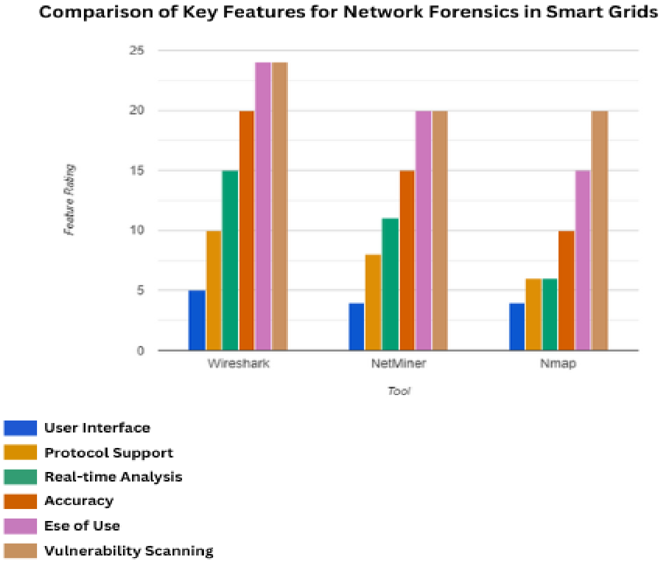


Figure 7. Comparative Analysis of Wireshark, NetMiner, Nmap

IV. RESULT ANALYSIS AND DISCUSSION

The network forensics tools, specifically Wireshark, NetMiner, and Nmap, offer a comprehensive analysis of their strengths and weaknesses in conducting forensic analysis in smart grid environment's post-fault incidents. The tool Comparison gives a broader outlook on their capabilities. Wireshark is renowned for its extensive protocol support and real-time analysis capabilities; it excels in accurate packet analysis and detailed network traffic insights. Its user-friendly interface and VoIP analysis features make it effective for immediate data interception and decryption.

However, the tool's complexity and resource consumption can present challenges for users. NetMiner stands noteworthy for its automatic file extraction and message extraction capabilities, it simplifies specific forensic tasks. While excelling in areas like file extraction protocols, it may lack Wireshark's manual packet analysis precision. Its ease of use is enhanced by focusing on specific tasks like message extraction. Nmap is recognized for its accuracy in network scanning and auditing tasks, it provides detailed information about network hosts and services. Its port scanning capabilities and OS detection features enhance precision in identifying vulnerabilities. However, Nmap's primary focus on network scanning may limit its usability for in-depth packet analysis compared to Wireshark

In terms of Ease of Use, Wireshark offers a user-friendly interface with real-time analysis capabilities but requires a solid understanding of network protocols. NetMiner simplifies specific tasks with automatic file extraction but may lack versatility in manual packet analysis.

Nmap provides a straightforward network scanning utility but may not offer as much depth in packet analysis compared to Wireshark.

V. CONCLUSION AND FUTURE WORK

Cyberattacks against critical electrical infrastructure pose a significant threat. Network forensics is pivotal in detecting, investigating, and understanding these malicious acts. By utilizing advanced tools and techniques to analyze network traffic and logs, investigators can gain crucial insights, identify perpetrators, and strengthen cybersecurity posture to safeguard the power grid. While Wireshark stands out for its real-time analysis capabilities and detailed insights, NetMiner simplifies specific tasks with automatic extraction features. On the other hand, Nmap's strength lies in accurate network scanning but may lack the depth of packet analysis compared to Wireshark. Each tool brings unique advantages to the table, catering to different aspects of network forensics post-fault incidents in smart grid environments. Understanding the specific use cases where each tool excels is crucial for leveraging their strengths effectively in forensic investigations within smart grid environments. Ultimately, the choice of tool depends on the specific requirements of the investigation, balancing factors like ease of use, accuracy, precision, and recall ensuring a comprehensive and effective forensic analysis process.

The future work extension of this domain would be to investigate the latest advancements in network forensics tools, such as real-time analysis capabilities, machine learning algorithms, and cloud-based solutions. This could include evaluating new tools and comparing their effectiveness in network forensics post-fault incidents in smart grid environments.

REFERENCES

[1] M. Surya, J. Sidabutar and N. Qomariasih, "Comparative Analysis of Recovery Tools For Digital Forensic Evidence Using NIST Framework 800-101 R1," 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 2023, pp. 258-262, doi: 10.1109/ICoCICs58778.2023.10276447.

[2] A. Tanner, F. C. Dancer, J. Hall, N. Parker, R. Bishop and T. McBride, "The Need for Proactive Digital Forensics in Addressing Critical Infrastructure Cyber Attacks," 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2022, pp. 976-982, doi: 10.1109/CSCI58124.2022.00174.

[3] F. Mohammed, N. A. A. Rahman, Y. Yusof and J. Juremi, "Automated Nmap Toolkit," 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 2022, pp. 1-7, doi: 10.1109/ASSIC55218.2022.10088375.

[4] J. Asokan, K. R. A. Britto, P. Valarmathi, M. S. Prakash Balaji, G. Sasi and V. Elamaran, "A Case Study Using National e-Government Portals to Investigate the Deployment of the Nmap Tool for Network Vulnerability Assessment," 2023 Second International Conference on Trends in Electrical, Electronics, and Computer Engineering (TEECCON), Bangalore, India, 2023, pp. 166-171, doi: 10.1109/TEECCON59234.2023.10335785.

[5] G. R. Sathi, L. Vedullapalli, M. H. Kishan, T. S. Zaman, M. T. Islam and M. M. Badr, "NetMiner: Identifying Failure-Inducing Patterns in the Logs Generated by Network Monitoring Software," 2023 14th International Conference on Computing Communication and Networking Technologies (ICT), Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10308051.

[6] J. Asokan, A. K. Rahuman, B. Suganthi, S. Fairooz, M. S. P. Balaji and V. Elamaran, "A Case Study Using Companies to Examine the Nmap Tool's Applicability for Network Security Assessment," 2023 12th International Conference on Advanced Computing (ICoAC), Chennai, India, 2023, pp. 1-6, doi: 10.1109/ICoAC59537.2023.10249544.

[7] K. Touloumis, A. Michalitsi-Psarrou, A. Georgiadou and D. Askounis, "A tool for assisting in the forensic investigation of cyber-security incidents," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 2630-2636, doi: 10.1109/BigData55660.2022.10020208.

[8] Solanke, A.A., Biasiotti, M.A. Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. Künstl Intell 36, 143–161 (2022). https://doi.org/10.1007/s13218-022-00763-9

[9] J. Pärssinen, P. Raussi, S. Noponen, M. Opas and J. Salonen, "The Digital Forensics of Cyber-Attacks at Electrical Power Grid Substation," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800831.

[10] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," in IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[11] Delija, Damir & Mohenski, Ivan & Sirovatka, Goran. (2021). Comparative Analysis of Network Forensic Tools on Different Operating Systems. 1231-1235. 10.23919/MIPRO52101.2021.9596833.

[12] Qureshi, Sirajuddin & Qureshi, Saima & Akhtar, Faheem & Wajahat, Ahsan & Nazir, Ahsan & Ullah, Faheem. (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.

[13] Barik, K., Das, S., Konar, K., Chakrabarti Banik, B., & Banerjee, A. (2021). Exploring user requirements of network forensic tools. Global Transitions Proceedings, 2(2), 350-354. https://doi.org/10.1016/j.gltp.2021.08.043

[14] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, doi: 10.1109/COMST.2019.2962586.

[15] I. Kotsiuba, I. Skarga-Bandurova, A. Giannakoulias and O. Bulda, "Basic Forensic Procedures for Cyber Crime Investigation in Smart Grid Networks," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 4255-4264, doi: 10.1109/BigData47090.2019.9006215.

[16] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015

[17] Paruchuri, S., Case, A., & Richard, G. G. (2020). Gaslight revisited: Efficient and powerful fuzzing of digital forensics tools. Computers & Security, 97, 101986. https://doi.org/10.1016/j.cose.2020.101986

[18] A. Iqbal, A. Shalaginov and F. Mahmood, "Intelligent analysis of digital evidence in large-scale logs in power systems attributed to the attacks," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 3088-3093, doi: 10.1109/BigData.2018.8622220.

[19] Rima Asmar Awad, Saeed Beztchi, Jared M. Smith, Bryan Lyles, and Stacy Prowell. 2018. Tools, Techniques, and Methodologies: A Survey of Digital Forensics for SCADA Systems. In Proceedings of the 4th Annual Industrial Control System Security Workshop (ICSS '18). Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3295453.3295454

[20] Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. International Journal of Critical Infrastructure Protection, 18, 20-33. https://doi.org/10.1016/j.ijcip.2017.07.002

[21] K. Clemente and E. Hesla, "Two Electrical Forensic Engineering Case Studies," in IEEE Transactions on Industry Applications, vol. 50, no. 6, pp. 4197-4201, Nov.-Dec. 2014, doi: 10.1109/TIA.2014.2346706.

[22] C. S. Mardegan and D. Shipp, "Anatomy of a complex electrical failure and its forensics analysis," 2013 IEEE Industry Applications Society Annual Meeting, Lake Buena Vista, FL, USA, 2013, pp. 1-10, doi: 10.1109/IAS.2013.6682593.

[23] W. -H. Chuang, R. Garg and M. Wu, "Anti-Forensics and Countermeasures of Electrical Network Frequency Analysis," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2073-2088, Dec. 2013, doi: 10.1109/TIFS.2013.2285515.

[24] B. A. Allaf, "Power system monitoring and analysis," 2010 IEEE International Energy Conference, Manama, Bahrain, 2010, pp. 297-301, doi: 10.1109/ENERGYCON.2010.5771695.

[25] Nai Fovino, I., Guidi, L., Masera, M., & Stefanini, A. (2011). Cyber security assessment of a power plant. Electric Power Systems Research, 81(2), 518-526. https://doi.org/10.1016/j.epsr.2010.10.012

[26] Yoke-Lin Tan, "Damage of a distribution transformer due to through-fault currents: an electrical forensics viewpoint," 2001 IEEE Industrial and Commercial Power Systems Technical Conference. Conference Record (Cat. No.01CH37226), New Orleans, LA, USA, 2001, pp. 121-126, doi: 10.1109/ICPS.2001.966521.

[27] https://www.smart-energy.com/industry-sectors/cybersecurity/energy-cybersecurity-in-2024-building-accountability-and-responsibility/

[28] https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/?sh=513704b3101a

[29] https://electrical-engineering-portal.com/electric-power-systems

[30] https://www.elprocus.com/overview-smart-grid-technology-operation-application-existing-power-system/

[31] Hasan, Mohammad Kamrul & Habib, A K M & Islam, Shayla & Safie, Nurhizam & sheikh abdullah, Siti & Sheikh, Huda & Pandey, Bishwajeet. (2023). ScienceDirect DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Reports. 9. 29-31. 10.1016/j.egyr.2023.05.184.