SUMMER TRAINING REPORT

On

“Cyber Security Manager Internship at ANZ”

Submitted in partial fulfillment of the requirements for the

award of the degree of

Bachelor of Technology

in

Computer Science Engineering

with specialization in

Cyber Security

Submitted by

Utkarsh Pandey (202210101180005)

Under the supervision of

Mr. Manish Srivastava

Assistant Professor

Department of Computer Science & Engineering

Shri Ramswaroop Memorial University

Lucknow – Deva Road, Barabanki (Uttar Pradesh)

DECLARATION

I, Utkarsh Pandey, a student of Bachelor of Technology in Computer Science & Engineering with specialization in Cyber Security, VIIth semester, in Shri Ramswaroop Memorial University hereby declare that this *Summer Training Report* entitled "Cyber Security Manager Internship at ANZ" is an outcome of my own work carried out during my internship period.

The work presented here is genuine, conducted under the supervision and mentorship of professionals from Forage and ANZ, Australia. The report has not been submitted elsewhere for the award of any other degree or diploma.

Date: November 1, 2025

Place: Lucknow

Signature: _____

Name: Utkarsh Pandey

CERTIFICATE

This is to certify that Utkarsh Pandey, a student of Bachelor of Technology in Computer Science Engineering, VIIth Semester, Shri Ramswaroop Memorial University, has successfully completed an internship at Australia and New Zealand Banking Group Limited (ANZ, Australia) as part of the academic requirement.

The internship took place from June 4, 2025, to July 4, 2025, during which the student worked in the role of Cyber Security Manager. Throughout this period, he was responsible for monitoring and analyzing web traffic and investigating network log files using advanced tools such as Wireshark. His duties included identifying potential security threats, analyzing anomalies in network patterns, and ensuring the integrity and safety of ANZ's digital infrastructure.

We hereby confirm that the student has fulfilled the internship requirements as prescribed by the university.

Date: _____

Signature of Supervisor
Department of Computer Science Engineering
Shri Ramswaroop Memorial University

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Forage for giving me the invaluable opportunity to provide me internship with ANZ Australia as Cyber Security Manager. This internship has been a crucial milestone in my academic and professional journey, allowing me to bridge the gap between theoretical knowledge and practical industry applications.

First and foremost, I extend my sincere thanks to Cholena Orr, Graduate Program Manager at ANZ, for her guidance throughout the internship period. Her patience, detailed explanations, and practical insights not only enhanced my technical skills but also helped me develop confidence in handling real-world incidents.

I would also like to acknowledge the Forage and ANZ support teams for being easily approachable and supportive. Their spirit, timely feedback, and willingness to share knowledge contributed significantly to my learning.

I am thankful to my faculty members and institution mentors, who encouraged me to pursue this internship and provided academic support, ensuring that I could apply classroom training effectively in the professional environment.

CERTIFICATE OF COMPLETION

ANZ

Forage

Inspiring and empowering future professionals

Utkarsh Pandey

Cyber Security Management Job Simulation

Certificate of Completion

July 4th, 2025

Over the period of July 2025, Utkarsh Pandey has completed practical tasks in:

Social Engineering Investigation
Digital Investigation

Cholena Orr
Graduate Program Manager, ANZ

Tom Brunskill
CEO, Co-Founder of Forage

Enrolment Verification Code mFLM9545wpSDjSWL3 | User Verification Code GsJSPvo552xfPs3gA | Issued by **Forage**

CONTENT

1. INTRODUCTION

The internship program is an integral part of the Bachelor of Technology curriculum, designed to provide students with real-world exposure to industrial environments and practical applications of academic knowledge. It bridges the gap between theoretical learning and professional practices followed by the industry. This summer training has been an enriching experience that enabled me to gain valuable insights into the field of Cyber Security and its implementation in real organizational settings.

I had the privilege of completing my internship at Australia and New Zealand Banking Group Limited (ANZ, Australia) through Forage Virtual Internship Program, where I worked in the role of a Cyber Security Manager. During this internship, I was exposed to various real-life scenarios involving web traffic monitoring, network log investigation, and digital forensics. The training allowed me to practically apply my classroom knowledge in areas such as network security, data integrity, and incident analysis.

The main objective of this internship was to understand how a large financial institution like ANZ ensures the security and confidentiality of its digital infrastructure against evolving cyber threats. By working with professional tools such as Wireshark and analyzing real-time network patterns, I learned to identify anomalies, detect potential intrusions, and take preventive measures to safeguard systems.

Through this internship, I developed a deeper understanding of the operational side of cybersecurity management, including the process of analyzing web traffic, investigating log files, and generating evidence-based reports for threat assessment. This experience not only strengthened my technical foundation but also enhanced my analytical thinking and problem-solving abilities.

2. ORGANIZATION PROFILE

Australia and New Zealand Banking Group Limited (ANZ) is one of the largest and most reputable financial institutions in the Asia-Pacific region. Headquartered in Melbourne, Australia, ANZ operates in more than 30 markets worldwide, serving over 8.5 million customers across retail, commercial, and institutional banking sectors. The bank has established itself as a global leader in providing innovative financial solutions, risk management, and digital banking services.

Founded in 1835, ANZ has built a strong reputation for its commitment to customer trust, integrity, and technological advancement. The organization emphasizes sustainable growth, data-driven decision-making, and digital transformation to enhance its service delivery and security infrastructure. As a financial leader, ANZ continuously invests in advanced cybersecurity frameworks to protect customer data and ensure the integrity of its digital operations.

The Cyber Security Division at ANZ plays a critical role in safeguarding the bank's assets, networks, and customer information from emerging threats. The division focuses on areas such as network monitoring, incident response, vulnerability assessment, threat intelligence, and risk mitigation. By integrating cutting-edge tools and methodologies, the team ensures that the organization remains resilient against evolving cyber threats and complies with global security standards.

ANZ's culture promotes innovation, learning, and ethical responsibility. The bank encourages young professionals and interns to engage in practical projects that simulate real-world challenges. Through programs like Forage Virtual Internship, it provides students with an opportunity to experience the work environment of a cybersecurity professional, gain exposure to enterprise-level tools, and understand the decision-making processes involved in protecting a global financial network.

Overall, ANZ's commitment to technological excellence and cybersecurity resilience makes it an ideal organization for aspiring cybersecurity professionals to learn, contribute, and grow.

3. INTERNSHIP OBJECTIVE

The primary objective of this internship was to gain practical exposure to the field of Cyber Security and understand its real-world applications within a global financial organization like Australia and New Zealand Banking Group Limited (ANZ). The internship was designed to bridge the gap between academic learning and professional industry practices by involving hands-on experience in security monitoring, analysis, and threat management.

The specific objectives of the internship were as follows:

1. To understand enterprise-level cybersecurity operations
   - Learn how large-scale organizations monitor and secure their digital infrastructure against potential cyber threats.

2. To analyze and interpret network traffic patterns
   - Gain the ability to use tools like *Wireshark* to identify anomalies, intrusions, and suspicious activities within a network.

3. To investigate and correlate network log files
   - Develop skills in examining and interpreting log data to detect patterns indicative of unauthorized access or breaches.

4. To familiarize with real-world incident handling procedures
   - Understand how cybersecurity teams respond to and mitigate network incidents in real-time environments.

5. To enhance technical proficiency in cybersecurity tools and methodologies
   - Acquire knowledge of professional tools, frameworks, and best practices used in the industry.

6. To develop analytical and problem-solving skills
   - Apply theoretical cybersecurity concepts to practical problems, enhancing decision-making and situational awareness.

7. To gain exposure to professional ethics and organizational security policies
   - Understand the importance of confidentiality, data protection, and adherence to compliance standards in financial institutions.
   - Prepare for future roles in cybersecurity through experiential learning and practical engagement with industry processes.

4. ROLE AND RESPONSIBILITIES

During my internship at Australia and New Zealand Banking Group Limited (ANZ) through Forage Virtual Internship Program, I served in the capacity of a Cyber Security Manager (Intern). The role primarily focused on understanding, monitoring, and safeguarding digital systems from potential cyber threats by analyzing real-time data and implementing preventive strategies.

As part of this role, I was responsible for a range of technical and analytical tasks that contributed to the protection and reliability of ANZ's network infrastructure. The following were my key roles and responsibilities during the internship.

4.1. Monitoring Network Traffic

- Observed live and simulated network traffic to identify irregularities and potential indicators of compromise.
- Ensured continuous vigilance of inbound and outbound data flow within secure network segments.

4.2. Analyzing Web Traffic Patterns

- Examined HTTP/HTTPS requests to detect suspicious behavior or malicious activities targeting the organization's web assets.

4.3. Investigating Network Log Files

- Utilized tools such as *Wireshark* to analyze packet captures and logs for signs of anomalies or policy violations.

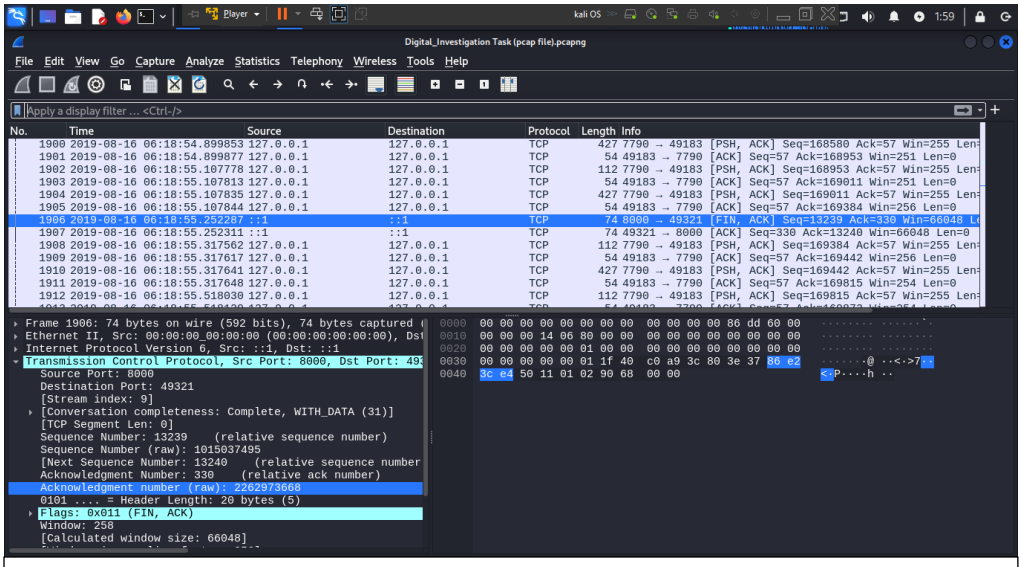


Figure 4.3.1. Snapshot of Wireshark analysis

- Correlated data from multiple sources to verify and trace the origin of potential incidents.

4.4. Identifying and Assessing Security Threats

- Detected potential cyber threats through pattern recognition, anomaly detection, and behavior analysis.
- Reported findings with evidence and recommended corrective or preventive measures.

4.5. Regenerating Evidence for Incident Analysis

- Extracted and reconstructed relevant network events from raw log data to support forensic examination and reporting.

4.6. Preparing Analytical Reports

- Documented observations, technical findings, and interpretations in structured reports to support internal review and audit processes.

4.7. Learning and Applying Security Protocols

- Understood and followed standard security procedures, data handling policies, and ethical guidelines maintained by ANZ.

---

5. TECHNICAL SKILLS

During my internship at ANZ, I developed several hands-on technical skills in the domain of Cyber Security and Network Analysis. The training provided a practical foundation for understanding how enterprise-level systems are secured, monitored, and analyzed against potential cyber threats.

The following are the major technical skills and tools I learned and applied during the internship:

5.1. Network Traffic Analysis using Wireshark

- Captured and analyzed live packet data using *Wireshark* to identify abnormal network patterns and possible intrusions.
- Applied protocol filters (HTTP, TCP, UDP, DNS, etc.) to isolate suspicious traffic and understand packet behavior.
- Traced IP flow, latency, and packet retransmission to diagnose potential security concerns.

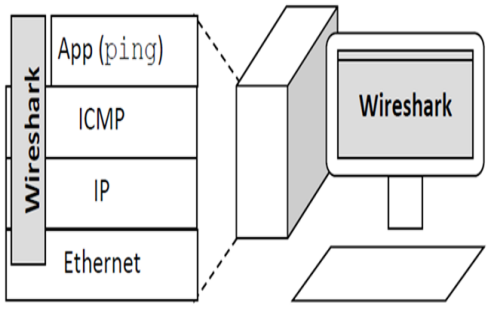


Figure 5.1.1. Demonstration of Wireshark capturing network packets

5.2. Command-Line Operations (CMD and Bash)

- Used *Windows Command Prompt (CMD)* and *Linux Bash terminal* for executing diagnostic commands like ping, tracert, netstat, and nslookup.
- Automated certain repetitive tasks and file operations using Bash scripting to streamline log analysis.

```
C:\Users\300058>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Blessings:0            LISTENING
  TCP    0.0.0.0:445            Blessings:0            LISTENING
  TCP    0.0.0.0:902            Blessings:0            LISTENING
  TCP    0.0.0.0:912            Blessings:0            LISTENING
  TCP    0.0.0.0:3306           Blessings:0            LISTENING
  TCP    0.0.0.0:5040           Blessings:0            LISTENING
  TCP    0.0.0.0:5357           Blessings:0            LISTENING
  TCP    0.0.0.0:8000           Blessings:0            LISTENING
  TCP    0.0.0.0:8089           Blessings:0            LISTENING
  TCP    0.0.0.0:8191           Blessings:0            LISTENING
  TCP    0.0.0.0:33060          Blessings:0            LISTENING
  TCP    0.0.0.0:49664          Blessings:0            LISTENING
  TCP    0.0.0.0:49665          Blessings:0            LISTENING
  TCP    0.0.0.0:49666          Blessings:0            LISTENING
  TCP    0.0.0.0:49667          Blessings:0            LISTENING
  TCP    0.0.0.0:49668          Blessings:0            LISTENING
  TCP    0.0.0.0:49674          Blessings:0            LISTENING
  TCP    127.0.0.1:2765         kubernetes:8191        ESTABLISHED
  TCP    127.0.0.1:2766         kubernetes:8191        ESTABLISHED
```

Figure 5.2.1. Demonstration of netstat command

```
C:\Users\300058>ping google.com

Pinging google.com [172.217.24.78] with 32 bytes of data:
Reply from 172.217.24.78: bytes=32 time=215ms TTL=111
Reply from 172.217.24.78: bytes=32 time=941ms TTL=111
Reply from 172.217.24.78: bytes=32 time=129ms TTL=111
Reply from 172.217.24.78: bytes=32 time=146ms TTL=111

Ping statistics for 172.217.24.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 129ms, Maximum = 941ms, Average = 357ms
```

Figure 5.2.2. Demonstration of ping command

5.3. Linux and Kali Linux Environment

- Worked in *Kali Linux*, a security-focused distribution widely used in ethical hacking and forensics.
- Navigated Linux file systems, handled permissions, and executed commands for monitoring network activity and handling logs.
- Learned the importance of Linux-based tools and open-source utilities in cybersecurity analysis.

5.4. Log File Investigation

- Examined system and network logs to detect unauthorized activities and anomalies.

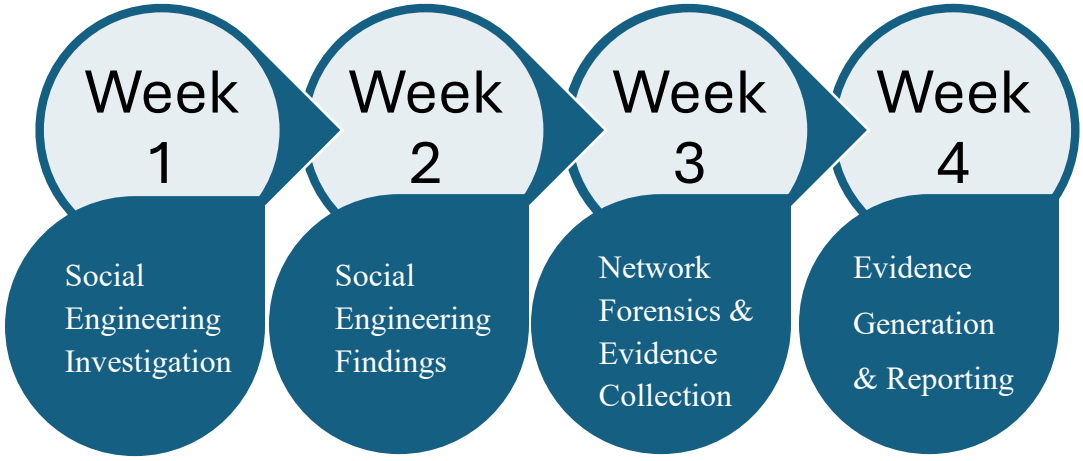
- Used text-processing tools (grep, cat, less, awk) to filter and interpret large log files efficiently.

5.5. Incident Response and Documentation

- Understood the standard steps in incident handling detection, analysis, containment, and reporting.
- Prepared structured reports highlighting findings, technical observations, and recommended mitigations.

---

6. INTERNSHIP TIMELINE



Week	Focus Area	Key Tasks Performed	Findings / Outcomes
Week 1	Social Engineering Investigation	Reviewed ANZ's *"How to Stay Safe Online"* guidelines; analyzed phishing samples for fake login URLs, mismatched headers,	Identified phishing indicators such as urgent tone, spoofed sender domains, and fake login links.

Week	Focus Area	Key Tasks Performed	Findings / Outcomes
		and malicious attachments.	Preserved email headers and artifacts.
Week 2	Social Engineering Findings	Examined 5 to 6 suspicious emails with fake domains and malware-laced attachments. Extracted IoCs (domains, IPs, hashes).	Documented incidents, detected *Invoice.pdf.exe* payload, recommended domain blocking and MFA verification steps.
Week 3	Network Forensics & Evidence Collection	Captured network packets using Wireshark, CMD, and Kali Linux tools. Applied filters (http, dns, ftp), used Follow TCP Stream and HTTP Object Extraction, viewed ASCII data, and analyzed streamed data.	Found repeated HTTP POST requests to unknown domains suggesting possible credential harvesting or malware beaconing.
Week 4	Evidence Generation & Case Documentation	Exported packets and objects, verified with SHA256 hashes, and mapped to MITRE ATT&CK (T1056,	Produced verified forensic evidence (.pcap, IPs, hashes, screenshots) and

Week	Focus Area	Key Tasks Performed	Findings / Outcomes
		T1041). Created event timeline and report.	documented final conclusions.

Table 6.1: 4-week internship Timeline

7. LEARNING OUTCOMES

The internship at Australia and New Zealand Banking Group Limited (ANZ) proved to be an enriching experience that significantly contributed to my academic, professional, and personal development. It provided me with a deeper understanding of how cybersecurity principles are implemented in a real-world environment and how theoretical concepts from classroom learning are applied to practical scenarios.

The key learning outcomes from the internship are as follows:

7.1. Practical Exposure to Cybersecurity Operations

Gained firsthand experience in monitoring and analyzing network traffic, investigating incidents, and identifying potential threats using industry-standard tools.

7.2. Proficiency in Network and Log Analysis

Learned to interpret packet data and system logs to detect irregularities, suspicious activities, and intrusion attempts within a network.

7.3. Understanding of Threat Detection and Response

Understood the complete process of identifying, analyzing, and mitigating cybersecurity threats in a financial organization's environment.

7.4. Technical Familiarity with Professional Tools

Developed working proficiency with Wireshark, Kali Linux, CMD, and Bash terminal for performing network diagnostics, data filtering, and forensic analysis.

7.5. Application of Theoretical Knowledge

Successfully applied concepts from academic courses such as Computer Networks, Cryptography, and Network Security in real-time problem-solving tasks.

7.6. Analytical and Critical Thinking Skills

Improved my ability to logically evaluate network patterns, trace root causes of anomalies, and make data-driven conclusions.

7.7.Professional Documentation and Reporting

Learned to maintain structured analytical reports, summarize observations clearly, and present findings in a professional format.

7.8. Adaptability and Independent Learning

Enhanced self-learning abilities through virtual internship modules, adapting quickly to new tools, environments, and task requirements.

7.9. Awareness of Industry Practices and Ethics

Understood the importance of confidentiality, compliance, and responsible data handling in cybersecurity operations within financial institutions.

8. CHALLENGES AND SOLUTIONS

Challenges	Solutions
• Difficulty in interpreting raw packet data and identifying meaningful information during initial Wireshark sessions.	Explored the **"Follow TCP Stream"** feature in *Wireshark* to visualize complete communication between endpoints and reconstruct conversations in ASCII format. Also used **"Export HTTP Objects"** for extracting web content and analyzing HTTP streaming behavior.
• Large and complex network log files made it difficult to filter relevant data manually.	Applied **Linux terminal commands** such as grep, awk, and cut for targeted filtering. Combined results with Wireshark filters (e.g., ip.addr == x.x.x.x) to isolate malicious activity efficiently.
• Limited experience with Bash scripting and Linux-based forensic workflows.	Referred to **Kali Linux documentation** and practiced common network commands like netstat, tcpdump, and ifconfig.

9. INTERNSHIP ACHIEVEMENTS

The major achievements during the internship are as follows:

9.1. Successful Completion of ANZ's Cyber Security Manager Virtual Internship

- Completed the virtual internship via Forage platform, performing all assigned tasks in phishing analysis, network forensics, and evidence generation aligned with ANZ's cybersecurity framework.

9.2.Detection of Phishing and Malware Activities

- Identified multiple simulated phishing attempts and malicious attachments through header inspection and domain analysis. Extracted Indicators of Compromise (IoCs) such as spoofed sender addresses, fake URLs, and encoded payloads.

9.3.Advanced Network Forensic Analysis using Wireshark

- Conducted in-depth packet analysis to trace abnormal traffic patterns across HTTP, DNS, and TCP protocols. Utilized Follow TCP Stream, Export HTTP Objects, and ASCII analysis features to reconstruct communication flows and detect credential harvesting attempts.

9.4.Digital Evidence Collection and Preservation

- Successfully exported **.pcap** files, generated SHA256 file hashes, and compiled timeline-based evidence suitable for forensic validation and reporting. Maintained evidence integrity as per digital forensics standards.

9.5.Mapping Threat Behavior with MITRE ATT&CK Framework

- Correlated observed anomalies with specific techniques such as T1056 (Input Capture) and T1041 (Exfiltration Over C2 Channel) to understand adversarial tactics and threat intelligence practices.

9.6.Report Writing and Documentation Skills

- Learned to draft professional vulnerability reports, clearly outlining the identified issue, its impact, root cause, and recommended mitigation measures. This enhanced my technical communication and report presentation abilities.

9.7.Independent Analytical and Diagnostic Work

- Worked autonomously using Wireshark, CMD, and Kali Linux, overcoming technical challenges through research, testing, and logical troubleshooting in a virtual environment.

9.8.Development of Professional Cybersecurity Awareness

- Acquired an understanding of enterprise-level defense systems, compliance obligations, and best practices for protecting sensitive financial data.

10. COMPARISON WITH ACADEMIC LEARNING

The internship experience at Australia and New Zealand Banking Group Limited (ANZ) provided valuable practical exposure that complemented and extended the theoretical concepts learned during the Bachelor of Technology in Computer Science and Engineering program. While classroom education provided a strong foundation in principles and frameworks, the internship transformed those concepts into real-world applications and operational understanding.

The following points highlight the comparison between academic learning and practical exposure:

10.1. From Theory to Application

Academic courses such as Computer Networks, Cybersecurity, and Cryptography and Network Security introduced the fundamental concepts of protocols, encryption, and data protection. During the internship, I applied these concepts using tools like Wireshark and Kali Linux to monitor, analyze, and secure network traffic.

10.2. Understanding Real-World Threats

While academics primarily focus on standard models and definitions of cyber threats, the internship exposed me to realistic attack scenarios such as phishing, malware injection, and credential harvesting. This practical exposure helped in understanding how these threats manifest in live environments.

10.3. Hands-on Experience with Industry Tools

In university labs, the focus remained on conceptual experiments. In contrast, the internship demanded the use of professional-grade tools such as Wireshark, CMD, and Bash for live data analysis, packet inspection, and evidence generation, bridging the gap between education and industry practice.

11. FUTURE SCOPE

The key areas of future scope identified from this internship are as follows:

1. Advanced Network Forensics and Threat Hunting
2. Integration of Machine Learning in Cybersecurity
3. Developing Automated Forensic Reporting Systems
4. Expanding Expertise in Cloud and Endpoint Security
5. Contributing to Open-Source Cybersecurity Communities

---

12. CONCLUSION

The internship was highly enriching and insightful experience that bridged the gap between academic learning and real-world application in the field of Cybersecurity and Network Forensics. It provided an opportunity to explore how theoretical knowledge from university courses could be effectively implemented to detect, analyze, and mitigate real-world security threats.

Throughout the internship, I gained practical experience in network traffic analysis, phishing investigation, log examination, and digital evidence generation using tools such as Wireshark, Kali Linux, CMD, and Bash. The tasks carried out during the four-week program ranging from social engineering analysis to forensic evidence documentation, it helped me understand the end-to-end process of cybersecurity operations in an enterprise environment.

---

13. REFERENCES

- **Australia and New Zealand Banking Group Limited (ANZ).** (2024). *How to Stay Safe Online – Protect Yourself.* Retrieved from https://www.anz.com.au/security/protect-yourself/online/
- **TheForage.** (2024). *ANZ Cyber Security Virtual Experience Program.* Retrieved from https://www.theforage.com/virtual-experience/programs/anz-cybersecurity
- **Wireshark Foundation.** (2024). *Wireshark User Guide & Documentation.* Retrieved from https://www.wireshark.org/docs/
- **MITRE Corporation.** (2024). *MITRE ATT&CK Framework – Enterprise Matrix.* Retrieved from https://attack.mitre.org/

- **Kali Linux Documentation.** (2024). *Kali Linux Tools and Command Reference.* Retrieved from https://www.kali.org/docs/
- **PacketTotal.** (2024). *Online PCAP Analysis and Malware Detection Platform.* Retrieved from https://packettotal.com/
- Stallings, W. (2019). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson Education.
- Forouzan, B. A. (2017). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.

14. APPENDIX

14.1. Appendix A – Incident Report submitted to ANZ for suspicious network activity

Incident Report: Analysis of Suspicious Network Activity

Date: July 4, 2025
Analyst: Utkarsh Pandey

Objective
Investigate suspicious network activity captured in pcap file "Digital_Investigation Task (pcap file).pcapng".

Methodology:

- Opened **Digital_Investigation Task (pcap file).pcapng** file in Wireshark
- Applied display filter: **http**
- Used **File → Export Objects → HTTP** to extract all HTTP-transferred files.
- Located file named **anz-logo.jpg** and **bank-card.jpg**

Findings:

File	URL/ Path	Timestamp	Source IP	Destination IP	Content -Type
anz-logo.jpg	http://localhost:8000/anz-logo.jpg	2019-08-16 06:17:40.663205	::1	::1	image/jpeg
bank-card.jpg	http://localhost:8000/bank-card.jpg	2019-08-16 06:17:58.633690	::1	::1	image/jpeg
ANZ1.jpg	http://localhost:8000/ANZ1.jpg	2019-08-16 06:19:37.273939	::1	::1	image/jpeg
ANZ2.jpg	http://localhost:8000/ANZ2.jpg	2019-08-16 06:19:49.666267	::1	::1	image/jpeg

14.2. **Appendix B -** Screenshot and Visual Evidence

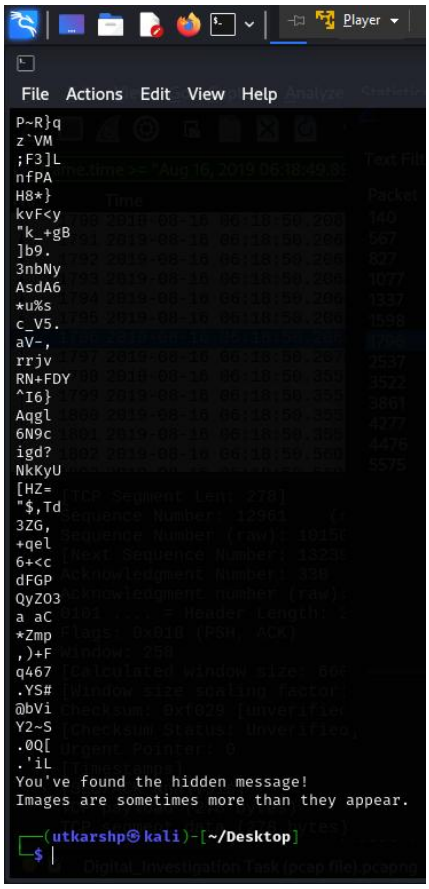


Figure 14.2.1 – Extraction of text hidden inside "Document.pdf" file

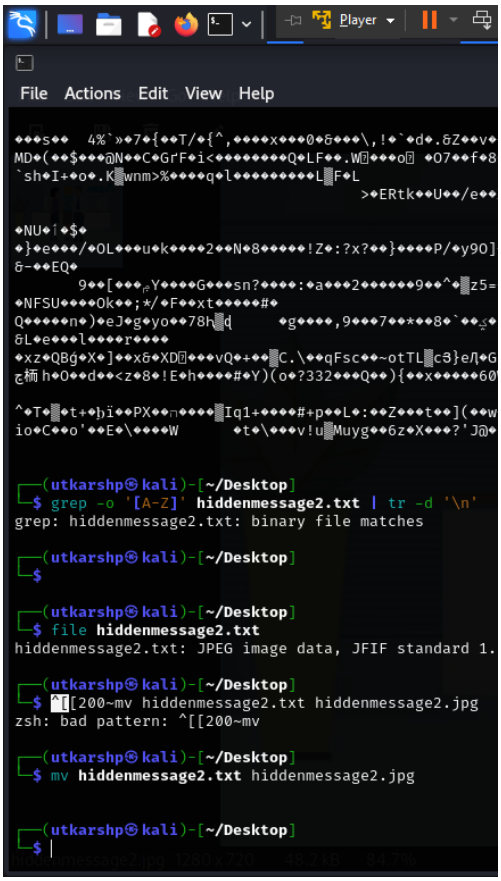


Figure 14.2.2 – Extraction of content of file "hiddenmessage2.txt"

14.3. **Appendix C -** Extraction and decoding of an image hidden inside a file "broken.png" as ASCII text of the original image.

Extracted image from ASCII text from broken image

```
┌──(utkarshp㉿kali)-[~/Desktop]
└─$ file broken.png
broken.png: ASCII text

┌──(utkarshp㉿kali)-[~/Desktop]
└─$ mv broken.png broken.txt

┌──(utkarshp㉿kali)-[~/Desktop]
└─$ mv broken.txt broken.png

┌──(utkarshp㉿kali)-[~/Desktop]
└─$ man head

┌──(utkarshp㉿kali)-[~/Desktop]
└─$ head broken.png
iVBORw0KGgoAAAANSUhEUgAAAZAAAAGQCAYAAACAvzbMAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJ
bWFnZVJlYWR5ccllPAAAEjBJREFUeNrs3d1RHMfaAOCyA46AhggQAR46QrCOgg
EYAisHzLjdYRHE4E2i+Cjy+Db5sZSpYsYGFnut+eZ6qxa6d+evrrvvvrrtt/+maQAAAA
```