NETWORK TRAFFIC ANALYSIS USING WIRESHARK AND ZEEK

MADE BY-- KARTIK KUMAR
COLLEGE--DRONACHARYA GROUP OF
INSTITUITIONS, GREATER NOIDA
COUSE NAME—IBM PBEL/CYBERSECURITY
DATE- 30/7/2025
SUPERVISOR- NIKHIL PANDEY

Abstract





• In today's digital age, network security has become a critical concern, with threats ranging from malware intrusions to unauthorized access attempts. This beginner-level project aims to address the challenge of identifying and analyzing suspicious activities within a network using powerful open-source tools—Wireshark and Zeek. By monitoring sample network traffic and applying custom analysis scripts, the project demonstrates how even basic setups can yield meaningful insights into network behavior.

- Wireshark was used to capture live packet data, enabling detailed inspection of protocols and communication patterns. Zeek
 complemented this process by extracting high-level logs and generating contextual alerts based on traffic anomalies. Together, these tools facilitated the detection of suspicious activities such as port scanning, unusual connection attempts, and data exfiltration behaviors.
- The project provides a curated GitHub repository containing sample datasets, analysis scripts, logs, and a conclusive summary of observed threats. The results highlight how early-stage network monitoring can play a vital role in strengthening cybersecurity awareness. Overall, this hands-on project serves as an introduction to practical network forensics and encourages further exploration into proactive threat detection methods.

Table of Content

Topic	Page No.		
Abstract	2-3		
Introduction	5-6		
Literature Review	7-8		
Methodology	9-13		
Result and Discussion	13-15		
Conclusion	16-17		
References	18		
Appendices	19-24		

INTRODUCTION

- What's the project about? This project focuses on monitoring and analyzing network traffic to identify suspicious activities and potential threats. Using basic but powerful tools, it introduces the fundamentals of network security through hands-on investigation.
- Why this project? Why is it important? Cyber threats are constantly evolving, and
 even small networks can be vulnerable to attacks. I chose this project to learn how to
 detect unusual patterns that may indicate hacking attempts or data breaches.
 Understanding the basics of network forensics is a crucial first step toward building
 stronger digital defenses.

 How will it be solved? I captured network traffic using Wireshark and analyzed logs and events with Zeek. By studying packet details and connection behaviors, I was able to pinpoint suspicious activities and understand what normal traffic should look like versus abnormal behavior.

5

Tools and techniques used

- Wireshark for capturing and inspecting live packet data.
- **Zeek** for generating logs, detecting anomalies, and summarizing network events.
- Custom scripts and sample datasets to assist with deeper analysis and visualization.

LITERATURE REVIEW

- Existing Technologies & Research This project is built on widely recognized tools and practices in network security analysis.
- Wireshark, a leading packet analysis tool, is frequently cited in cybersecurity literature for protocol inspection and traffic diagnostics.
- Zeek (formerly Bro) is a versatile network monitoring framework used in academic research and enterprise threat detection systems.

- Sources & Reference Material In addition to tool documentation and community forums, I referred to the official Wireshark website to access sample datasets and educational resources. These materials played a key role in shaping the project's methodology and validating its findings.
- Why These Tools? Both tools offer extensive community support and proven effectiveness in identifying anomalies. Leveraging their combined strengths allowed for a comprehensive and hands-on approach to understanding network behavior and threat patterns.

METHODOLOGY

- ➤ **Project Approach** The goal was to detect suspicious network behavior using beginner-friendly tools. I followed a step-by-step plan:
 - Data Collection: Gathered network traffic samples using Wireshark and from its official website.
 - Traffic Inspection: Used Wireshark to examine packet-level data and highlight unusual patterns.
 - Log Analysis: Implemented Zeek to generate structured logs from traffic, enabling deeper insight.
 - Scripting & Investigation: Ran custom scripts to scan logs for anomalies like port scanning or odd IP behavior.
 - Conclusion & Reporting: Identified key findings and compiled results into GitHub for transparency and review.

>Tools & Technologies Used

- Wireshark: A packet capture tool that lets users visually inspect individual network packets, including protocols, source/destination IPs, and payloads.
- **Zeek**: A high-level network analysis tool that converts traffic into searchable logs, helping identify security-relevant events.
- Sample Datasets: Included both captured data and Wireshark-sourced examples to simulate realistic scenarios.
- **Python Scripts**: Wrote basic filters and alerts to sift through Zeek logs for signs of abnormal traffic.

➤ Step-by-Step Process

- Installed Wireshark and zeek
 - Downloaded and installed Wireshark and zeek on my local machine (Windows/Linux/macOS)
 - Granted appropriate permissions for packet capture
- Selected Network Interface
 - •Chose the active network interface (e.g., Wi-Fi or Ethernet) to begin capturing live data
 - Ensured the interface was actively transmitting packets
- Captured Network Traffic
 - •Let Wireshark run for a set period to collect enough traffic samples
 - •Saved captured traffic in .pcap format for later analysis
- Filtered and Analyzed Packets
 - •Used built-in filters (e.g., http, dns, tcp.port==80) to isolate relevant traffic
 - Inspected specific packets for unusual patterns, like large payloads or excessive SYN requests

11

Identified Suspicious Activity

- Observed anomalies such as repeated TCP connection attempts or malformed packets
- •Flagged potential indicators of scanning, spoofing, or unexpected outbound connections

Documented Findings

- Took screenshots of suspicious traffic
- Compiled notes explaining the protocol behavior and why it was suspicious
- Summarized the results in a project report

RESULTS AND DISCUSSIONS

- ➤ Results: After analyzing the captured network traffic using Wireshark, I discovered several noteworthy findings:
 - •Suspicious DNS Requests: There were repeated queries to domains that looked unusual or potentially malicious, such as those ending with uncommon TLDs.
 - •Unusual TCP Behavior: Wireshark revealed a flood of TCP SYN packets without matching ACK responses. This pattern might indicate a port scan attempt.
 - •Large Data Transfers: Outbound traffic spikes occurred during late hours when no active use was expected. This raised concerns about possible unauthorized data movement.
 - •Insecure Protocol Usage: Some web activity was conducted over unsecured HTTP connections. Sensitive details, such as login credentials, were visible in plain text within packet payloads.

> Discussion:

- The DNS activity suggests the possibility of beaconing behavior, where a compromised device periodically reaches out to command-and-control servers.
- TCP SYN flooding is often linked to reconnaissance activity by attackers trying to discover open ports.
- High outbound traffic during idle times could imply background services accessing external resources or potential exfiltration.
- Usage of HTTP over HTTPS presents security risks, especially if credentials or personal data are involved.

Challenges Faced:

- Interpreting the vast number of packets was overwhelming in the beginning.
- Certain protocols like TLS and ICMP were complex and required additional learning.
- Not every suspicious-looking packet was truly malicious—differentiating false positives from genuine threats took effort.
- Crafting precise Wireshark filters to narrow down relevant traffic patterns was a bit tricky but ultimately rewarding.

CONCLUSION

➤ Project Outcome: The project successfully met its goal of identifying and investigating suspicious network activity using Wireshark. By capturing live traffic, applying filters, and analyzing packet-level data, I was able to uncover key insights such as unsecured protocol use, unusual DNS queries, and potential port scanning behavior. This confirmed the effectiveness of Wireshark as a beginner-friendly tool for practical network forensics.

>What I Learned:

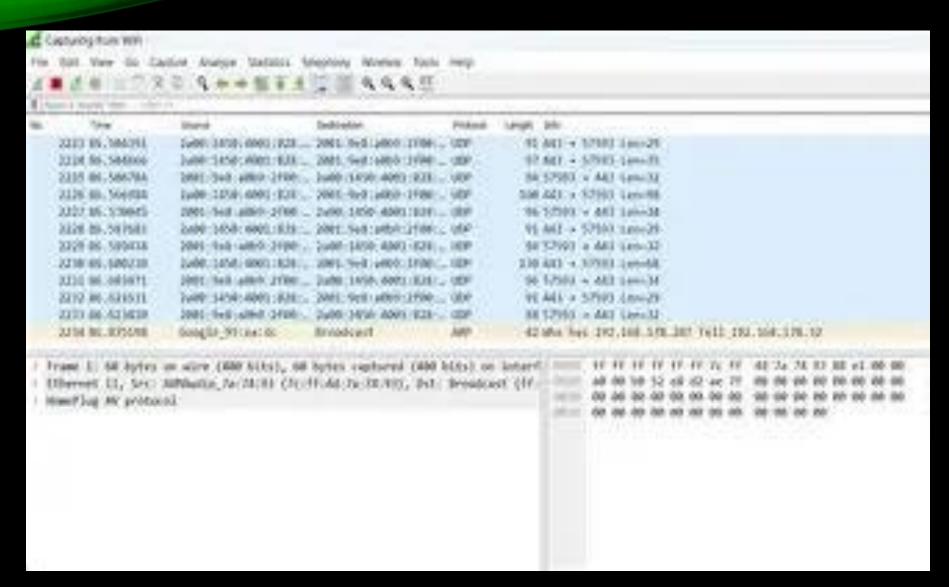
- How to use Wireshark to monitor and interpret live network traffic
- How different protocols behave under normal and abnormal conditions
- The importance of filtering and careful inspection to isolate meaningful data
- Basic signs of suspicious behavior such as SYN floods, odd DNS queries, and plaintext login data

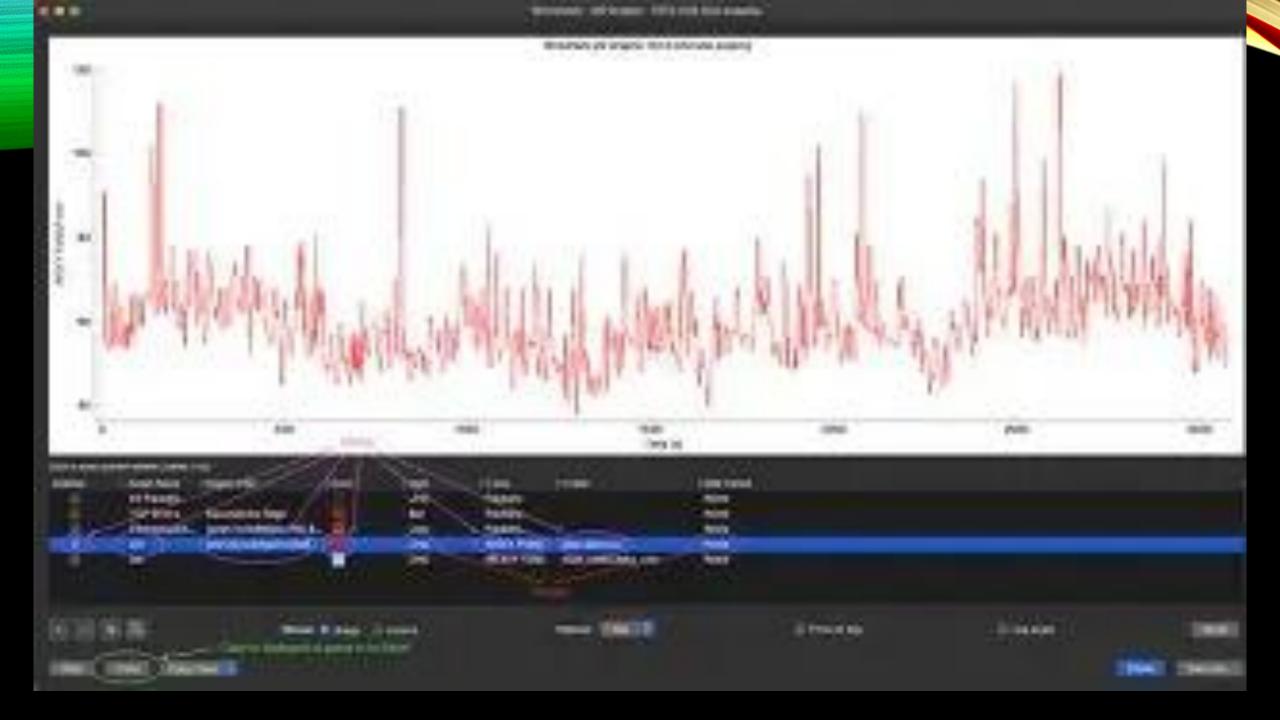
- Automate Analysis: Develop scripts to detect anomalies in captured traffic automatically
- Use Additional Tools: Combine Wireshark with tools like Zeek or Snort to enhance detection and logging capabilities
- Simulate Attacks: Set up a controlled environment to simulate attacks like DoS or phishing and study their network footprint
- Visual Reporting: Create dashboards or use Python visualization libraries to represent traffic patterns and findings more clearly

REFERENCES

- 1. Combs, G. (n.d.). Wireshark Network Protocol Analyzer. Retrieved from https://www.wireshark.org
- 2. Paxson, V. (n.d.). *Zeek Network Security Monitor (formerly Bro)*. Retrieved from https://zeek.org
- 3. Wireshark Foundation. (n.d.). Wireshark Sample Captures. Retrieved from https://wiki.wireshark.org/SampleCaptures
- 4. The Zeek Project. (n.d.). Zeek Documentation. Retrieved from https://docs.zeek.org
- 5. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.
- 6. Stallings, W. (2017). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional.

APPENDICES

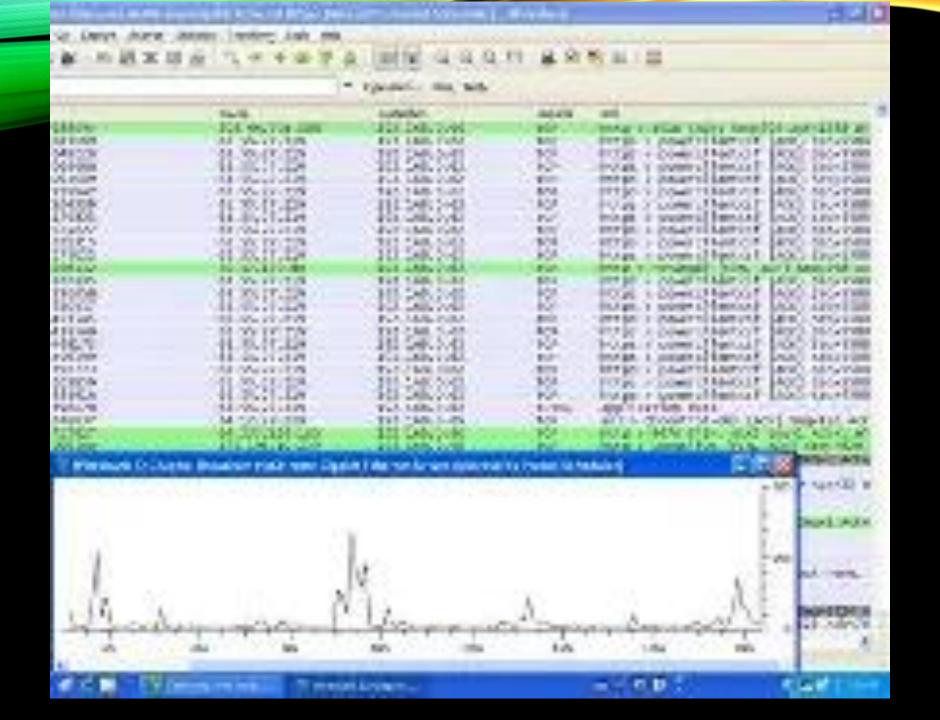




A COLUMN TWO IS NOT THE OWNER. Salve Male Water Stephen Territor Sen year 國際 电十二位下流 正 电电电阻 Debugger of Society 20.7 ATTENDED. PERSONAL PROPERTY. **KNOP** THE REAL PROPERTY. WHEN THE ARREST MARKET STREET S.A. Sales 3.4.34632 INC. INC. INC. E81-184-299-109 LOUIS STREET, N. HOTELS, E. 48-3640-144-140-04-1 \$190,100 FOLUM 5000 ATT TO MAKEN THE RESERVE A. of the special control 101-100-00-27 _ All Markey saids better a basepartic graphed our PROCESS AND THE If A SIGNE THE RECEIPT OF _ THE MANUFACTURE CONTRACTOR RESIDENCE TO SERVICE AND ADMINISTRACTOR OF A STATE OF THE SERVICE AND ADMINISTRATION OF THE SERVICE AND ADMINISTRAT DECIME LINES N. C. Bellins DESCRIPTION AND 180,008,146,17 m the following agency directly in checks below, and compare, one THE WHEN Chief. Distributed by the control babble is characterised and the field of a set of the babble THE RESERVE AND ADDRESS. \$40.084.546.481 25-540/205/207 MAKE: SEASON NAMED IN ASSTAGE AND NYCKEY'S DEPOS RELIGIO SHOWING BALANCE OR SCHOOL SERVICE 100,240,398.35 MINISTER, MICH. (MIX.) SHOWS MAKE MEMORIPHY LINES. 207/07/21/20 NO. \$4.9k TOMBUR 183, \$100, 504-45 DECIMAL DESCRIPTION TABLE THE PERSON NAMED IN AT IS A PERSON. 18 ft 15 / 19/- 88 ERFORD SIRE OF True! this set I have have your and Anne would be seen that the property of a recognition that THE REPORT OF PERSONS ASSESSED AND ADDRESS OF THE PARTY O AT SHIPPING DESCRIPTION OF REAL PROVINCES A 286 10A BY MADRICK MET, ALL COLUMN DOMESTICAL DESIGNATION OF THE PERSON OF THE 100 THE ME - TELLS LEDGE DEPOSES AND RESIDENCE AND ADDRESS OF THE PROPERTY OF A PRESIDENCE OF DA-BETT 183, \$5, \$50, 364 200/248-346/00 7754 sen sat v 1636 (43) hapony accord shocked onecks 554 agent of a recomment the AN ELECTRONIC 21.15.15.25 PW-185-150-05 107 VEHICLES A STREET SERVE MADERAL MADERAL ADDRESS AND VEHICLES AND ADDRESS OF A VANCOUS AND WEST THE A SERVICE STREET PRINTED THE PRINTED THE PRINTED STREET, THE PRINTED THE PRINTED STREET, THE PRINTED S DISCHARGE. 121 31 241 68 FEV. MAJOR, RI TEXAL COACH 251 John 200 VI DISCREEN AND -0 201 SERVE C 400 LINES Beg-180 Four Ribe IntroCKENA Union. TREAM DALKS DELWOOL ME 3094.00 14" Claric by Endings, Sings Chitel Sec., Astropas minima Terrigio 311,4004.0 185 Harge Curve Son, Incoder Salesbay No. 445 ARRESTS IN DEC. TH. LEW. OFF. PM-144-140-01 PATRICK. ALC: NO POST RE-175 200 Vale 25 507-W-HL 490 WHOM: WE SEARCH WITH COLD SOURCEST DESCRIPT GOVERNMENT WHITE II n. NOW TALESTON, MALES ARCHITICAL DRIV Published IIII Application (Mar-STATEMENT 105, 530, 566, 54 DE SCOTT AND TOTAL ST. TORY INVOLVED WITH SHIP. 14 15 1 15 15 16 21120 410,485 \$45,000 (MLG) . BOAL - 1206 1631 Non-felt machine recommend have HI CHINA MODEL PROJECT THE WALLESTON NAME OF TAXABLE PARTY. STREET, SQUARE STREET 223.045.0 DECEMBER 18-41 MEAN COLLARS OA. AND THE PART LAST, EMPORES ADDRESS, SENDICIPAL LAND DESCRIPTION. SECURIOR RESERVE XIV/MUSEUM Marie I DESCRIPTION ASSESSMENT TO SECURE THE SECURE ASSESSMENT SECURITY STREET, SALES SECURITY STREET, SALES SECURITY STREET, SALES THE RESERVE me DETAILS THE WAY THE WAY DESCRIPTION OF THE PERSON NAMED IN COLUMN TWO IN COLUMN TW MET SOCK SHE PROCESS ARRANGE FEB-4-31 THE ARREST OF THE PARTY. MIT JOHN 101-200-20-45 DOUBLESS. HQ# properly work 1801 horo more electricated 151-150-09-11 50.00 \$100 PHONESON PROPERTY. TIT SALPS MAKE DESCRIPTION DR NAME: TO LOURS WHILE T THE ASS. SEE 24. DRIVER SECTION THE SCHOOL P. ACCOUNT. DEEL AND THE RE N/Um THE PERSON NAMED IN DISCUSSION. Life John Strucker mi PK2012F00M 1012-140-200-87 100.04.1601 Or 15 project factors filed by a 15 percentages, proglements, com-390 WILLIAM COLD GFE 140, WE S. 19039-140-0 Michigan and antique service below a recovering a grapher to the high life and SECULIFICATION. \$5.456.00E-22 121-22-276-278 **SMP** THE R. LEWIS CO., LANSING, A. Select V Demoit SCHOOL

Chitto		tatistics Teleph		1.75			
	CNI+O	1下土口	三 6 6 6 11				
			Source	Destrutor	30905	Deploy	99
mp.		32,270837	ANTHORED, SEPTEMBE	Broadcast:			All
	CN+W	32,278685	AprockIn_52:F1:81	Broadcast	100000		N
	100000	132,498864	10.29.108.189	19.18.255.255	54911	54915	s w
	C84-5	132,400846	10.10.100.185	19.18,255.255	34915	14915	P 00
	Chin Shanis	33,493498	D0120.188.189	19.10.101.246	55701	144	5.TI
	-	133,370735	Asmoskin 52: Tirel	Browlest			Al
		13,278750	10.10.102.125	28-18-188-185	50000	1439	1
		133,492343	10.10.189.185	10.10.215.255	54915	54911	F. U
uts		133,490325	10.10.100.105	18.18.255.255	54915	54915	F-01
Epin-	~ ~ ~ ~	134,279051	10.20.100.155	18.19.106.155	51910	E-866.	ł 1)
		134,494399	10.10.100.105	18.16.255.255	-54915	54912	F, UI
	Cod+Shift+X	34,494413	18.18.188.185	18,18,255,255	50915	54835	E M
		135,492372	10.10.100.105	18.18.255.255	58011	54925	1 13
		35,492349	19,19,188,185	10.10.255.255	54915	54935	F UI
		136,373795	58.18.188.185	45.32.24.138	45954	5541	b U
	وأقالي ويبروي	36,492669	18,19,186,185	10.18.255.255	54915	34915	R 10
	Ctri+P	36,492887	19.18.188.185	18.18.255.255	54915	54913	5-U
		36,056549	45.32.24.338	10.18-108-105	55413	4595	6.46
	Chil+Q	198467,534	19-14-103-105	\$8.38.255.255	54915	1481	l U
		177 XTHON	10 10 100 100	58-38-305-305	8,00018	8.6977	6.34

A company				
to be ver to	SERVICE SHAPE SHE	OR OTHER DAY	100.00	
		主人口思考外		
Residence of				
a. ma	there	NAME OF THE PARTY	None	MAN PROCESSION OF THE PROPERTY
4 8 5750	11 5 5 1 10	100.000	100	THE PARTY WAS ARRESTED AND ADDRESS OF THE PARTY WAS ARRESTED ADDRESS OF THE PARTY WAS ARRESTED AND ADDRESS OF THE PARTY WAS ARRESTED AND ADDRESS OF THE PARTY WAS ARRESTED AND ADDRESS OF THE PARTY WAS ARRESTED ADDRESS OF THE PARTY WAS
12.1591	METERSON	D5.04 E.05	64.7	For the Contract Street, or September 517 and that there
1.000000	PT 84-5-50	MATERIAL PROPERTY.	800	AN THE VALUE OF THE BEAT DOOR SHARE IN VALUE
1.000000	MEASURE	15 55 4 55	Mile.	THE THE STREET STREET, SHOWING THE PART OF THE STREET,
15 600	PERMIT	BROWN STREET	86	on I be success the I have been been a proved by a week.
45,6500	M9-85-02781	BARRIES.	64	THE THE MARKING AMPLICATIONS SHOULD BE THE THE AMPLICATION.
100,00000	FEED 1.50	09/3 EU/10/01	80	the Talk State And the Experience segres (register) to a least
\$1.5 PAIN.	495.655.2251	PERMIT	600	THE THE REPORT OF THE PROPERTY OF THE PARTY AND ADDRESS.
143593.86	PERCENC	escalari, int	60	Of the day the partie of the property of the parties of the partie
12 5 2 5 5 5 5	APPLICATION OF	SASTEM.	950	THE THE PROPERTY AND ADDRESS OF THE PART ADDRESS.
16 5 6 990	T9363.00	- 20100014	60	OF THE CASE WICKER CORP (MAD CONTROLLED AND
11 7, 15, 25	AN 45-1-16	1545040	200	THE RESESSED OF THE PARTY OF TH
113-26-85	44.454.46	26-11-12	P.F.	U.M. J. JASSON CO. SALES AND CONTRACTOR CONT
174.0951	MARKAGIS	AN HATE	60.	THE REAL PROPERTY OF THE PROPE
13 4, 0004	1010010	26315-511	80.0	O. R Milkoyor State of Child Country State
315.008	- 49 15 0 31	1541440	10	AN WELL-AND LOSS SHEET WAS TO AND THE COMMENT AND AND THE
24-4, \$10.04	TATHE DE	- 24 18 COM	~	the Ministration and Styles Company and
I MODELL SOL BATTOL TYPING I WARRISTAN AND SOLAR STR. III JORGANIAN SOL SOLAR STR. III SOLAR SOLAR SOLAR SOLAR SOL	PARTY OF SHIRL THE OFFICE A COST OF THE PRODUCT COST OF THE COST THE PRODUCT COST OF THE PARTY COST OF THE PARTY THE PARTY COST OF THE PARTY COS	Carlotte Common Carlotte Common Carlotte Common Carlotte Common Carlotte Ca	MARY IN	an an aminology area.
			or street	
O'F MINNS	named to the Art. A print			Project NO Jenning Ind Social



THANK YOU!