# 📊 PCAP Extraction Guide for Emmanuel (Security Analyst)

## 🎯 Overview

This guide shows you how to convert Cowrie's JSON attack logs into PCAP files for network analysis in Wireshark.

---

## 🚀 Quick Start - Generate PCAP from JSON Logs

### \*\***Step 1: Connect to Honeypot**\*\*

```bash

*honeypot*

# *Or: ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47*

```

### \*\***Step 2: Run PCAP Conversion Script**\*\*

```bash

*cd* /opt/cowrie

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

```

This will generate: `/tmp/cowrie\_traffic.pcap`

---

## 📥 Download PCAP to Your Local Machine

### \*\***Option 1: Download Single PCAP**\*\*

```bash

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./cowrie\_analysis.pcap

```

### \*\***Option 2: Generate & Download in One Command**\*\*

```bash

*ssh* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py" && \

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./cowrie\_$(*date* +%Y%m%d).pcap

```

---

## 🔍 Advanced PCAP Generation

### \*\***Generate PCAP for Specific Date Range**\*\*

```bash

# *On EC2 instance*

*cd* /opt/cowrie

# *Filter JSON logs by date first*

*grep* "2025-10-2[0-3]" var/log/cowrie/cowrie.json > /tmp/filtered\_logs.json

# *Convert filtered logs to PCAP*

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/filtered\_logs.json /tmp/filtered\_traffic.pcap

```

### \*\***Generate PCAP for Specific Attacker IP**\*\*

```bash

# *Filter by specific IP*

*grep* "192.168.1.100" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/attacker\_logs.json

# *Convert to PCAP*

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/attacker\_logs.json /tmp/attacker\_traffic.pcap

```

### \*\***Generate PCAP for Specific Session**\*\*

```bash

# *Get session ID from logs*

SESSION\_ID="a1b2c3d4e5f6"

# *Filter by session*

*grep* "\"session\":\"$SESSION\_ID\"" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/session\_logs.json

# *Convert to PCAP*

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/session\_logs.json /tmp/session\_traffic.pcap

```

---

## 🔬 Analyze PCAP in Wireshark

### \*\***Open PCAP File**\*\*

1. Download PCAP to your local machine

2. Open Wireshark

3. File → Open → Select `cowrie\_analysis.pcap`

### \*\***Useful Wireshark Filters**\*\*

```

# Show only SSH traffic

tcp.port == 22 or tcp.port == 2222

# Show traffic from specific IP

ip.src == 192.168.1.100

# Show failed login attempts

ssh.message\_code == 51

# Show successful logins

ssh.message\_code == 52

# Show command execution

tcp.payload contains "bash" or tcp.payload contains "wget"

```

### \*\***Analysis Checklist**\*\*

- [ ] Identify attacker source IPs

- [ ] Analyze SSH handshake patterns

- [ ] Track command execution sequences

- [ ] Identify malware download attempts

- [ ] Document attack timeline

- [ ] Extract IOCs (Indicators of Compromise)

---

## 📊 Batch PCAP Generation for Analysis

### \*\***Generate Daily PCAPs**\*\*

```bash

# *On EC2 instance*

*for* day *in* {20..23}; *do*

*echo* "Generating PCAP for 2025-10-$day..."

*grep* "2025-10-$day" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/logs\_$day.json

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/logs\_$day.json /tmp/traffic\_2025-10-$day.pcap

*done*

# *Download all PCAPs*

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/traffic\_\*.pcap ./

```

### \*\***Generate Per-Attacker PCAPs**\*\*

```bash

# *Get top 10 attacker IPs*

TOP\_IPS=$(*grep* -o '"src\_ip":"[^"]\*"' /opt/cowrie/var/log/cowrie/cowrie.json | \

*sed* 's/"src\_ip":"//g' | *sed* 's/"//g' | *sort* | *uniq* -c | *sort* -nr | *head* -10 | *awk* '{print $2}')

# *Generate PCAP for each attacker*

*for* ip *in* $TOP\_IPS; *do*

*echo* "Generating PCAP for $ip..."

*grep* "\"src\_ip\":\"$ip\"" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/attacker\_${ip}.json

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/attacker\_${ip}.json /tmp/traffic\_${ip}.pcap

*done*

```

---

## 🛠️ Troubleshooting

### \*\***Script Not Found**\*\*

```bash

# *Check if script exists*

*ls* -la /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

# *If missing, check alternate location*

*find* /opt/cowrie -name "logs2pcap.py"

```

### \*\***Permission Denied**\*\*

```bash

# *Run with sudo*

*sudo* python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

# *Or fix permissions*

*sudo* chmod +x /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

```

### \*\***Python Dependencies Missing**\*\*

```bash

# *Install required packages*

*sudo* pip3 install scapy

```

### \*\***Large File Size**\*\*

```bash

# *Compress PCAP before download*

*gzip* /tmp/cowrie\_traffic.pcap

# *Download compressed file*

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap.gz ./

```

---

## 📈 Analysis Workflow for Emmanuel

### \*\***Weekly Analysis Routine**\*\*

1. \*\***Generate Weekly PCAP**\*\*

   ```bash

   ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py"

   ```

2. \*\***Download to Local**\*\*

   ```bash

   scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./analysis/week\_$(*date* +%U).pcap

   ```

3. \*\***Analyze in Wireshark**\*\*

   - Open PCAP file

   - Apply filters for suspicious activity

   - Document findings

4. \*\***Generate Report**\*\*

   - Top attacking IPs

   - Attack patterns identified

   - Malware samples detected

   - Recommendations

---

## 🎯 Key Metrics to Extract from PCAP

### \*\***Network Statistics**\*\*

- Total packets captured

- Unique source IPs

- Average session duration

- Peak attack times

### \*\***Attack Patterns**\*\*

- Brute force attempts (repeated login failures)

- Port scanning activity

- Malware download attempts

- Command execution sequences

### \*\***IOCs (Indicators of Compromise)**\*\*

- Malicious IP addresses

- Suspicious domains

- Malware file hashes

- Attack signatures

---

## 📚 Additional Resources

### \*\***Wireshark Documentation**\*\*

- [Wireshark User Guide](https://www.wireshark.org/docs/wsug\_html\_chunked/)

- [Display Filter Reference](https://www.wireshark.org/docs/dfref/)

### \*\***PCAP Analysis Tools**\*\*

- \*\***Wireshark**\*\*: GUI-based packet analyzer

- \*\***tshark**\*\*: Command-line packet analyzer

- \*\***tcpdump**\*\*: Packet capture utility

- \*\***NetworkMiner**\*\*: Network forensics tool

### \*\***Cowrie Documentation**\*\*

- [Cowrie GitHub](https://github.com/cowrie/cowrie)

- [Cowrie Output Plugins](https://cowrie.readthedocs.io/en/latest/output/output.html)

---

## 🚨 Quick Reference Commands

```bash

# *Generate PCAP*

*ssh* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py"

**📊 PCAP Extraction Guide for Emmanuel (Security Analyst)**

**🎯 Overview**

This guide shows you how to convert Cowrie's JSON attack logs into PCAP files for network analysis in Wireshark.

**🚀 Quick Start - Generate PCAP from JSON Logs**

**Step 1: Connect to Honeypot**

honeypot

# Or: ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47

**Step 2: Run PCAP Conversion Script**

cd /opt/cowrie

sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

This will generate: /tmp/cowrie\_traffic.pcap

**📥 Download PCAP to Your Local Machine**

**Option 1: Download Single PCAP**

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./cowrie\_analysis.pcap

**Option 2: Generate & Download in One Command**

ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py" && \

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./cowrie\_$(date +%Y%m%d).pcap

**🔍 Advanced PCAP Generation**

**Generate PCAP for Specific Date Range**

# On EC2 instance

cd /opt/cowrie

# Filter JSON logs by date first

grep "2025-10-2[0-3]" var/log/cowrie/cowrie.json > /tmp/filtered\_logs.json

# Convert filtered logs to PCAP

sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/filtered\_logs.json /tmp/filtered\_traffic.pcap

**Generate PCAP for Specific Attacker IP**

# Filter by specific IP

grep "192.168.1.100" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/attacker\_logs.json

# Convert to PCAP

sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/attacker\_logs.json /tmp/attacker\_traffic.pcap

**Generate PCAP for Specific Session**

# Get session ID from logs

SESSION\_ID="a1b2c3d4e5f6"

# Filter by session

grep "\"session\":\"$SESSION\_ID\"" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/session\_logs.json

# Convert to PCAP

sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/session\_logs.json /tmp/session\_traffic.pcap

**🔬 Analyze PCAP in Wireshark**

**Open PCAP File**

1. Download PCAP to your local machine
2. Open Wireshark
3. File → Open → Select cowrie\_analysis.pcap

**Useful Wireshark Filters**

# Show only SSH traffic

tcp.port == 22 or tcp.port == 2222

# Show traffic from specific IP

ip.src == 192.168.1.100

# Show failed login attempts

ssh.message\_code == 51

# Show successful logins

ssh.message\_code == 52

# Show command execution

tcp.payload contains "bash" or tcp.payload contains "wget"

**Analysis Checklist**

* Identify attacker source IPs
* Analyze SSH handshake patterns
* Track command execution sequences
* Identify malware download attempts
* Document attack timeline
* Extract IOCs (Indicators of Compromise)

**📊 Batch PCAP Generation for Analysis**

**Generate Daily PCAPs**

# On EC2 instance

for day in {20..23}; do

  echo "Generating PCAP for 2025-10-$day..."

  grep "2025-10-$day" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/logs\_$day.json

  sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/logs\_$day.json /tmp/traffic\_2025-10-$day.pcap

done

# Download all PCAPs

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/traffic\_\*.pcap ./

**Generate Per-Attacker PCAPs**

# Get top 10 attacker IPs

TOP\_IPS=$(grep -o '"src\_ip":"[^"]\*"' /opt/cowrie/var/log/cowrie/cowrie.json | \

  sed 's/"src\_ip":"//g' | sed 's/"//g' | sort | uniq -c | sort -nr | head -10 | awk '{print $2}')

# Generate PCAP for each attacker

for ip in $TOP\_IPS; do

  echo "Generating PCAP for $ip..."

  grep "\"src\_ip\":\"$ip\"" /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/attacker\_${ip}.json

  sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/attacker\_${ip}.json /tmp/traffic\_${ip}.pcap

done

**🛠️ Troubleshooting**

**Script Not Found**

# Check if script exists

ls -la /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

# If missing, check alternate location

find /opt/cowrie -name "logs2pcap.py"

**Permission Denied**

# Run with sudo

sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

# Or fix permissions

sudo chmod +x /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py

**Python Dependencies Missing**

# Install required packages

sudo pip3 install scapy

**Large File Size**

# Compress PCAP before download

gzip /tmp/cowrie\_traffic.pcap

# Download compressed file

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap.gz ./

**📈 Analysis Workflow for Emmanuel**

**Weekly Analysis Routine**

1. **Generate Weekly PCAP**    ```bash

   ssh -i ~/.ssh/gmu-honeypot-key.pem [ec2-user@44.218.220.47](mailto:ec2-user@44.218.220.47) "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py"    ```

1. **Download to Local**    ```bash

   scp -i ~/.ssh/gmu-honeypot-key.pem [ec2-user@44.218.220.47](mailto:ec2-user@44.218.220.47):/tmp/cowrie\_traffic.pcap ./analysis/week\_$(date +%U).pcap    ```

1. **Analyze in Wireshark**    - Open PCAP file    - Apply filters for suspicious activity    - Document findings
2. **Generate Report**    - Top attacking IPs    - Attack patterns identified    - Malware samples detected    - Recommendations

**🎯 Key Metrics to Extract from PCAP**

**Network Statistics**

* Total packets captured
* Unique source IPs
* Average session duration
* Peak attack times

**Attack Patterns**

* Brute force attempts (repeated login failures)
* Port scanning activity
* Malware download attempts
* Command execution sequences

**IOCs (Indicators of Compromise)**

* Malicious IP addresses
* Suspicious domains
* Malware file hashes
* Attack signatures

**📚 Additional Resources**

**Wireshark Documentation**

* [Wireshark User Guide](https://www.wireshark.org/docs/wsug_html_chunked/)
* [Display Filter Reference](https://www.wireshark.org/docs/dfref/)

**PCAP Analysis Tools**

* **Wireshark**: GUI-based packet analyzer
* **tshark**: Command-line packet analyzer
* **tcpdump**: Packet capture utility
* **NetworkMiner**: Network forensics tool

**Cowrie Documentation**

* [Cowrie GitHub](https://github.com/cowrie/cowrie)
* [Cowrie Output Plugins](https://cowrie.readthedocs.io/en/latest/output/output.html)

**🚨 Quick Reference Commands**

# Generate PCAP

ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "cd /opt/cowrie && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py"

# Download PCAP

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./

# Generate filtered PCAP (last 24 hours)

ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "grep '$(date +%Y-%m-%d)' /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/today.json && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/today.json /tmp/today.pcap"

# Download today's PCAP

scp -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/today.pcap ./analysis\_$(date +%Y%m%d).pcap

**✅ Checklist for Emmanuel**

* Verify SSH access to honeypot
* Confirm logs2pcap.py script exists
* Generate test PCAP file
* Download PCAP to local machine
* Open PCAP in Wireshark
* Apply basic filters
* Document initial findings
* Set up weekly analysis routine

**Questions? Contact Kevin or check the main Team-Log-Analysis-Guide.md**

# *Download PCAP*

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/cowrie\_traffic.pcap ./

# *Generate filtered PCAP (last 24 hours)*

*ssh* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47 "grep '$(*date* +%Y-%m-%d)' /opt/cowrie/var/log/cowrie/cowrie.json > /tmp/today.json && sudo python3 /home/ec2-user/AWSHoneypot/02-Deployment-Scripts/logs2pcap.py /tmp/today.json /tmp/today.pcap"

# *Download today's PCAP*

*scp* -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.218.220.47:/tmp/today.pcap ./analysis\_$(*date* +%Y%m%d).pcap

```

---

## ✅ Checklist for Emmanuel

- [ ] Verify SSH access to honeypot

- [ ] Confirm logs2pcap.py script exists

- [ ] Generate test PCAP file

- [ ] Download PCAP to local machine

- [ ] Open PCAP in Wireshark

- [ ] Apply basic filters

- [ ] Document initial findings

- [ ] Set up weekly analysis routine

---

\*\***Questions? Contact Kevin or check the main Team-Log-Analysis-Guide.md**\*\*