

Beijing Forest Studio  
北京理工大学信息系统及安全对抗实验中心



**Wireless**  
Attacks in WPA2

Traffic Dataset for Krack and Kr00k

PhD Student : Munna Md Minhazul Islam 蒙纳

导师: Professor LUO SENLIN

2025年09月27日



1

**Overview of WPA2  
and its significance**

2

**Attack Simulation  
& Methodology**

3

**WPA2-KKID Dataset**

4

**Model Training  
& Performance**

5

**Strength & Limitations**



T	目标	Public dataset of KRACK/Kr00k traffic; fill WPA2 dataset gap; support ML-based IDS research
I	输入	Raw pcap traffic from controlled testbed; 5.5 M+ frames; both normal and attack sessions; engineered features
P	处理	Simulate attacks; capture traffic; extract features; heuristically label (EAPOL replay for KRACK, zero-key frames for Kr00k); balance & clean data; train various ML models.
O	输出	Public WPA2-KKID dataset (pcap & CSV); 34 features; labeled normal/attack samples; open access for researchers; foundation for IDS development
P	问题	Before this work, publicly accessible datasets on KRACK and Kr00k vulnerabilities were virtually nonexistent; existing collections like AWID3 include multiple attacks but lack public availability and a fully described framework.
C	条件	Lab-based environment with single AP and limited clients; ~10-minute capture sessions; WPA2-Personal on 2.4 GHz; controlled but not diverse
D	难点	Detecting subtle attack signatures; accurate labeling; handling class imbalance; limited device diversity and real-world variability.
L	水平	Computers & Security, (JCR 1, CAS 2)

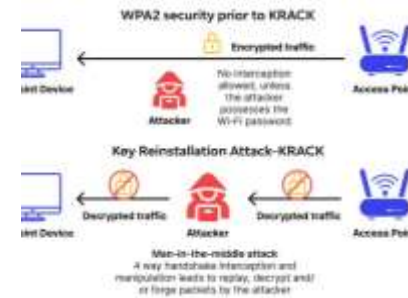
# Overview of WPA2 and its significance



## Encryption Strength

WPA2-Personal uses Advanced Encryption Standard (AES)

Public Wi-Fi hotspots, such as those in cafés and airports, commonly use WPA2-Personal due to its simplicity and ease of setup. However, this convenience comes with certain security risks, like susceptibility to man-in-the-middle attacks, especially if not combined with additional protections like a VPN.



## KRACK Attack: Real-World Exploitation

discovered in 2017



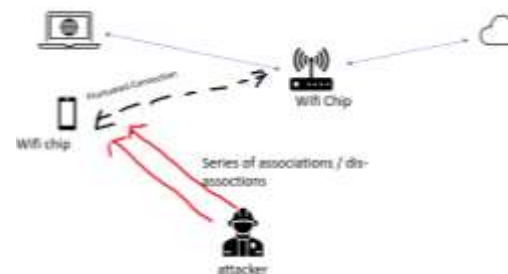
**Prevalence& Popularity** WPA2-Personal is the most common Wi-Fi security protocol worldwide

## How It Works

WPA2-Personal relies on the 4-way handshake and Pre-Shared Key (PSK) is used for authentication

## Kr00k Vulnerability

identified in 2019



To protect against WPA2 vulnerabilities, it's essential to use strong, complex passwords, and switch to WPA3 if possible, as it offers better security. Utilizing a VPN can help encrypt traffic on unsecured networks, while regularly updating router firmware ensures protection against known vulnerabilities.

# Overview of WPA2 and its significance



	KRACK (Key Reinstallation Attack)	Kr00k (Key Zeroing Attack)
Attack level	Network-level attack	Device-level attack
How it works	KRACK exploits a flaw in the WPA2 4-way handshake by forcing a reinstallation of the encryption key, allowing attackers to intercept and decrypt network traffic.	When a device disconnects from Wi-Fi, the encryption key (used in WPA2) is reset to all zeros. An attacker can force this disconnect and capture encrypted packets, which now use a zero key, making them easy to decrypt.
Impact	Allows eavesdropping, packet injection, and in some cases, hijacking connections	Decryption of previously encrypted Wi-Fi traffic
Password exposure	No (PSK not revealed)	No (PSK not revealed)

# Overview of WPA2 and its significance



SL NO.	Attack	Normal Traffic	Malicious Traffic
1	Deauth	1,587,527	38,942
2	Disas	1,938,585	75,131
3	(Re)Assoc	1,838,430	5,502
4	Rogue_AP	1,971,875	1,310
5	Krack	1,388,498	49,990
6	Kr00k	2,708,637	186,173
7	SSH	2,428,688	11,882
8	Botnet	3,169,167	56,891
9	Malware	2,181,148	131,611
10	SQL Injection	2,595,727	2,629
11	SSDP	2,641,517	5,456,395
12	Evil Twin	3,673,854	104,827
13	Website spoofing	2,263,446	405,121

## AWID3 Dataset



Publicly available datasets for these two attacks are scarce.



The dataset contains 254 features, a majority of which have missing values (NaNs).



The raw dataset necessitates extensive cleaning before it can be used for machine learning.



The traffic generation framework lacks documentation for ensuring reproducibility.



The documentation lacks any description of the feature selection or data labeling methodologies.

# Overview of WPA2 and its significance



## Devices and Tools for the Test bed

Node	Brand	OS	CPU/RAM	IP Address	MAC Address
Access Point (Wireless Router)	ASUS RT-AC68U	Linux 3.0.0.4.386_51733	Dual-core 800 MHz	192.168.3.2	0C:8D:98:23:SE:21
Windows STA (Desktop)	Custom	Windows 10 Pro (20H2)	Core i5, 8GB DDR4	192.168.3.45	D4:25:8B:E2:8F:92
Mobile STA (Smartphone)	iPhone 6s	iOS 14.2	Apple A9, 2GB	192.168.3.24	88:55:B5:55:B2:D6
Attacker (Laptop)	HP Omen 15	Kali Linux 2024.4	Core i7, 16GB	192.168.3.113	2C:DB:07:14:D3:BD
Mobile STA (Smartphone)	Samsung Note 4	Android 6.0.2	Snapdragon, 3GB	192.168.3.139	A4:08:DC:3C:9A:01

File Name	Attacks	Attack Tools	Total Frames	Attack Frames	Duration
Krack	Channel MitM Attack, Key Reinstallation	Hostapd	1,656,984	289,424	5/10
Kr00k	TK Reinstallation	Aircrack-ng	3,625,550	677,812	5/10

## Test Bed

Attack Scenario & Packet Analysis



Approx. 10 minutes

Normal Traffic Capture  
Attack Traffic Capture

Capture Attack- Wireshark

eapol || wlan.fc.type\_subtype ==  
0x08

Tcpdump Analyzer

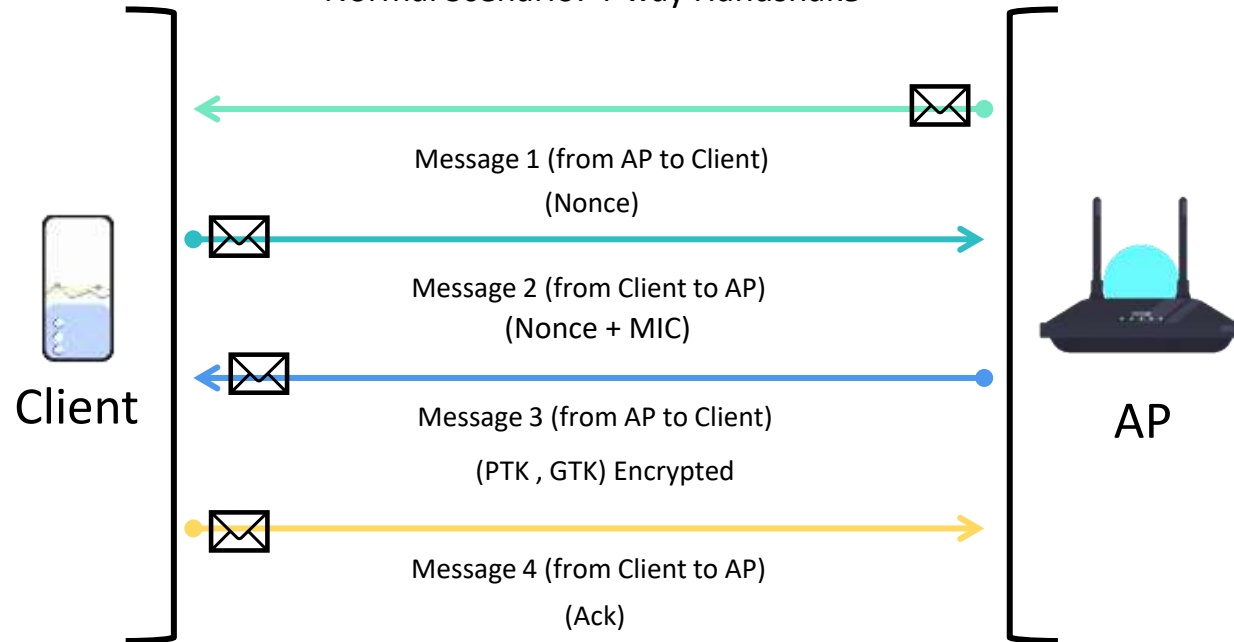
open source tcpdump to capture  
and analyze pcap files



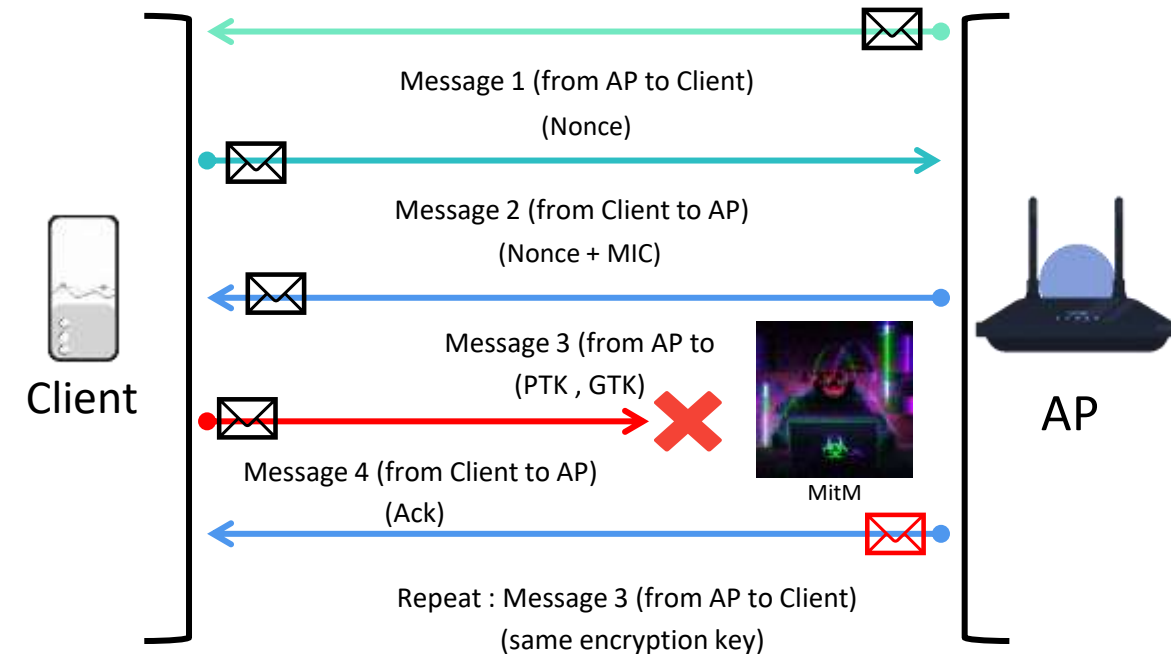
## KRACK Attack

Exploiting the 4-Way Handshake in WPA2

Normal Scenario: 4-way Handshake



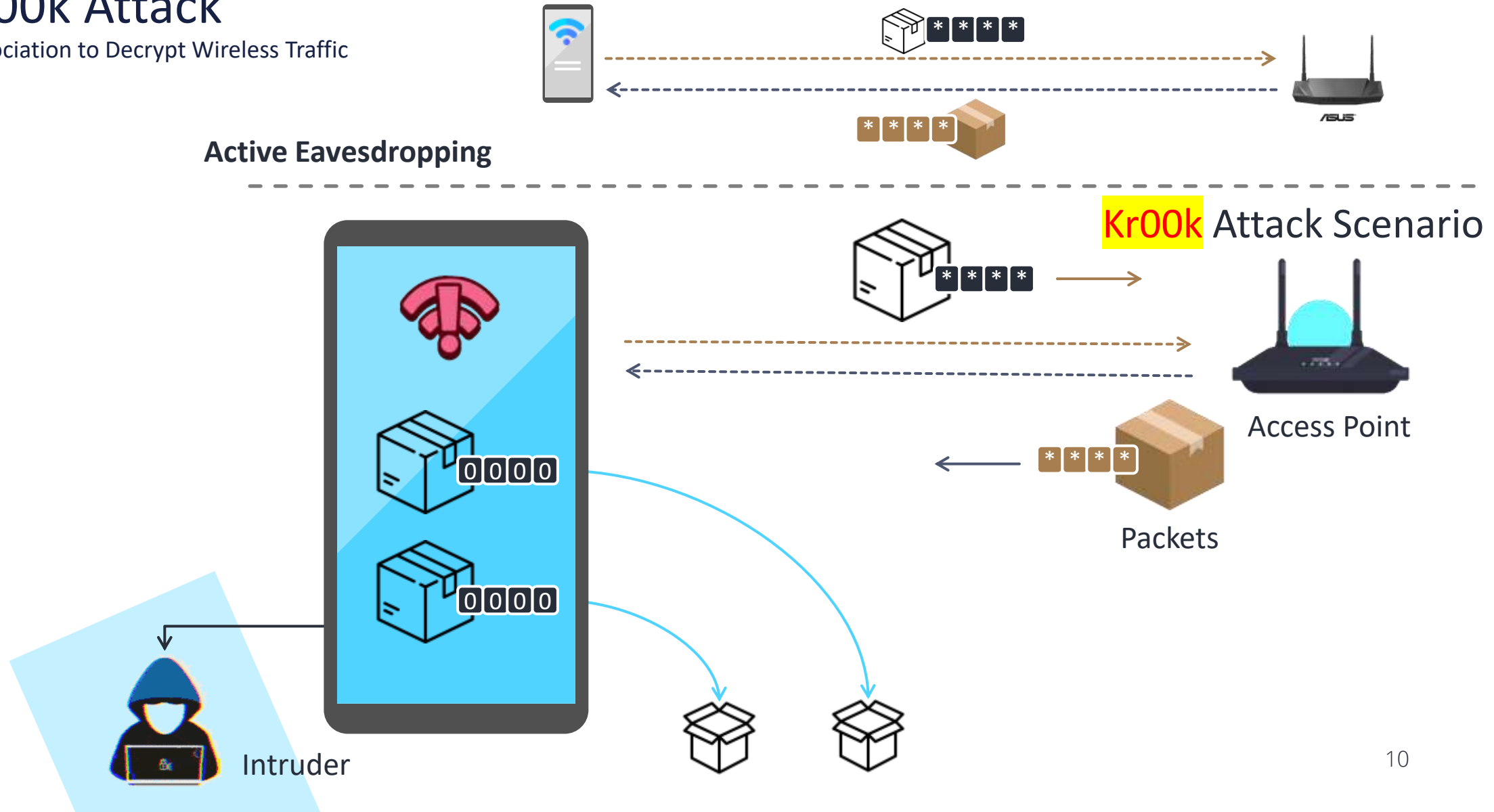
Krack Attack Scenario: 4-way Handshake



The attacker can now decrypt or manipulate traffic, breaking the security of WPA2 encryption.

## Kr00k Attack

Exploiting Disassociation to Decrypt Wireless Traffic



# Attack Simulation & Methodology



## Detecting KRACK Attacks in PCAP Files

Wireshark - Packet 1369931 - 5. Krack.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1368545	517.275919			EAP		102 Success
1368549	517.280542			EAPOL		215 Key (Message 1 of 4)
1368552	517.282539			EAPOL		215 Key (Message 2 of 4)
1368560	517.286526			EAPOL		281 Key (Message 3 of 4)
1368564	517.288439			EAPOL		193 Key (Message 4 of 4)
1369892	518.532735			EAPOL		215 Key (Message 1 of 4)
1369912	518.535171			EAPOL		237 Key (Message 2 of 4)
1369931	518.546219	ASUSTekCOMPU_54:fe:30	Alfa_a8:29:56	EAPOL		281 Key (Message 3 of 4)
1369932	518.548536	ASUSTekCOMPU_54:fe:30	Alfa_a8:29:56	EAPOL		281 Key (Message 3 of 4)

Wireshark - Packet 1369931 - 5. Krack.pcap

Frame 1369931: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)

Radiotap Header v0, Length 56

802.11 radio information

IEEE 802.11 QoS Data, Flags: .....F.C

Logical-Link Control

802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 183

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 3]

Key Information: 0x13ca

Key Length: 16

Wireshark - Packet 1369932 - 5. Krack.pcap

Frame 1369932: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits)

Radiotap Header v0, Length 56

802.11 radio information

IEEE 802.11 QoS Data, Flags: ....R.F.C

Logical-Link Control

802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 183

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 3]

Key Information: 0x13ca

Key Length: 16

## Detecting Kr00k Attacks in PCAP Files

kr0okappliedfilter.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ASUSTekCOMPU_54:fe:34	Broadcast	802.11	342	Beacon frame, SN=3062, FN=0, Flags=.....C, BI=100, SSID="ASUS_5G"

> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

> Radiotap Header v0, Length 56

> 802.11 radio information

▼ IEEE 802.11 Beacon frame, Flags: .....C

Type/Subtype: Beacon frame (0x0008)

▼ Frame Control Field: 0x8000

.... 00 = Version: 0

.... 00.. = Type: Management frame (0)

1000 .... = Subtype: 8

▼ Flags: 0x00

.... 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From D..

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

**.0.. .... = Protected flag: Data is not protected**

0... .... = +HTC/Order flag: Not strictly ordered

.000 0000 0000 0000 = Duration: 0 microseconds

> Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

> Transmitter address: ASUSTekCOMPU\_54:fe:34 (0c:9d:92:54:fe:34)

> Source address: ASUSTekCOMPU\_54:fe:34 (0c:9d:92:54:fe:34)

> BSS Id: ASUSTekCOMPU\_54:fe:34 (0c:9d:92:54:fe:34)

.... 0000 = Fragment number: 0

1011 1111 0110 .... = Sequence number: 3062

Frame check sequence: 0x2787e701 [unverified]

[FCS Status: Unverified]

[WLAN Flags: .....C]

> IEEE 802.11 Wireless Management

0000 00 00 38 00 2f 40 40 a0 20 08 00 a0 20 08 00 00 --8./@@- ... ..

0010 a0 9c 39 e0 01 00 00 00 10 0c 3c 14 40 01 de 00 --9.....< @-..

0020 00 00 00 00 00 00 00 00 8b 9c 39 e0 00 00 00 00 .....9.....

0030 16 00 11 03 d8 00 de 01 80 00 00 00 ff ff ff ff .....T-4...T-4^

0040 ff ff 0c 9d 92 54 fe 34 0c 9d 92 54 fe 34 60 bf .....-0-4-8-<-@

0050 3c d0 f1 cd 01 00 00 00 64 00 11 11 00 07 41 53 <.....d....AS

0060 55 53 5f 35 47 01 08 8c 12 98 24 b0 48 60 6c 05 US\_5G...-\$-H^1-

0070 04 02 03 00 00 07 34 44 45 20 24 01 17 28 01 17 .....4D E \$-(..

0080 2c 01 17 30 01 17 34 01 17 38 01 17 3c 01 17 40 ,..0-4-8-<-@

0090 01 17 64 01 1e 68 01 1e 6c 01 1e 70 01 1e 74 01 -d-h-1-p-t-

00a0 1e 84 01 1e 88 01 1e 8c 01 1e 00 20 01 00 23 02 .....-#-

00b0 12 00 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 --0.....

00c0 01 00 00 0f ac 01 8d 00 0b 05 00 00 01 00 00 2d .....-

00d0 1a ad 09 17 ff ff ff 00 00 00 00 00 00 00 00 .....-

00e0 00 00 00 00 00 00 00 00 00 00 00 3d 16 24 08 00 .....-\$.--

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....-

0100 00 00 00 7f 08 04 00 08 00 00 00 00 40 bf 0c b2 .....@-..

0110 59 82 0f ea ff 00 00 ea ff 00 00 c0 05 00 24 00 Y.....\$-

0120 00 00 c3 02 00 02 dd 09 00 10 18 02 00 00 9c 00 .....P-..-^

0130 00 dd 18 00 50 f2 02 01 88 00 03 a4 00 00 27 .....BC^b 2/-F-r-

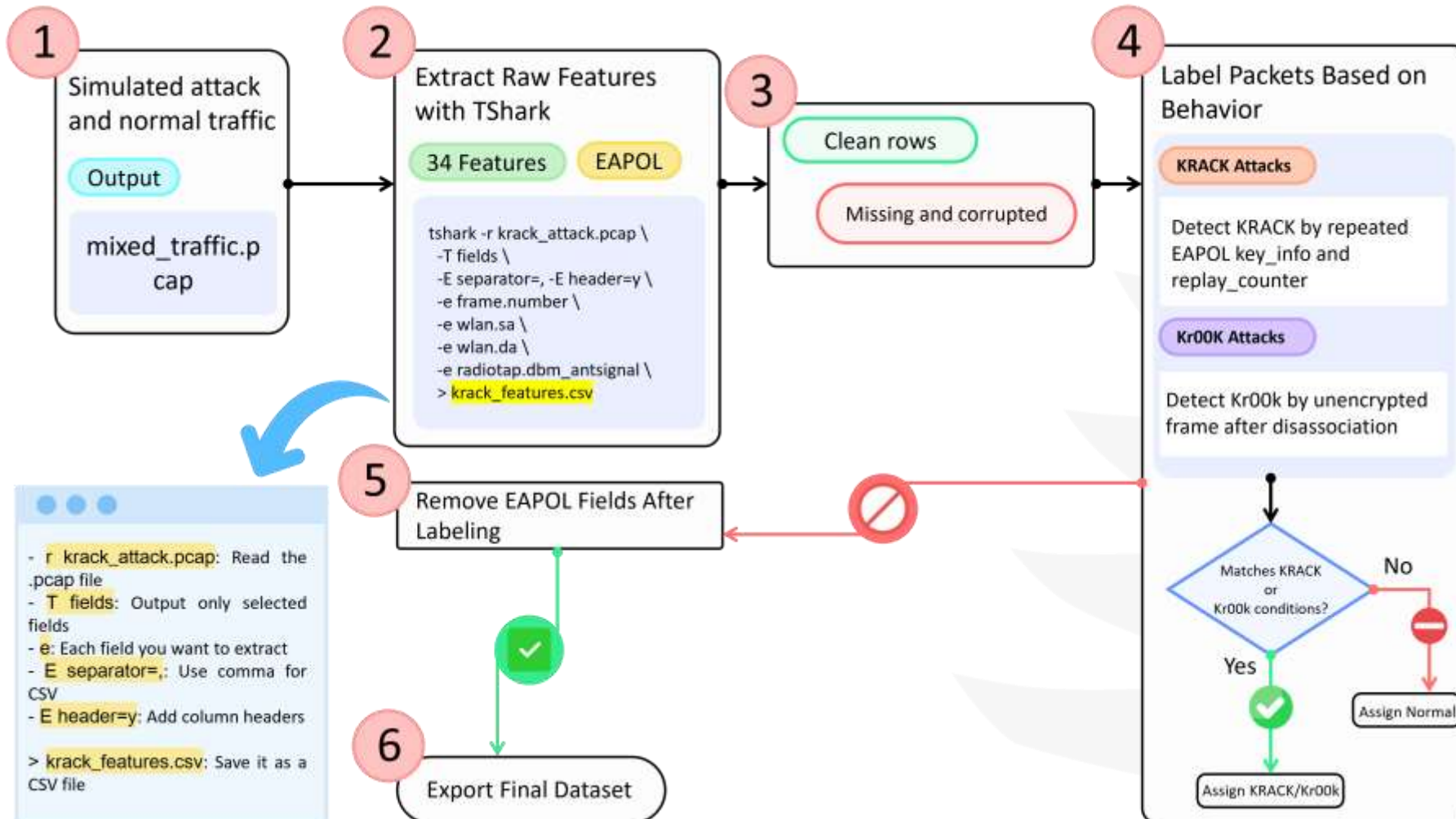
0140 a4 00 00 42 43 5e 00 62 32 2f 00 46 05 72 08 01 .....^

0150 00 00 01 e7 87 27

## Detecting Kr00k Attacks in PCAP Files

```
01:02:36.430505 5180 MHz 11a -36dBm signal User 0 MCS 6 LDPC FEC 20 MHz long GI [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.430509 8414441586us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] BA RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.430657 8414441745us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.430700 8414441788us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.431023 5180 MHz 11a -36dBm signal User 0 MCS 6 LDPC FEC 20 MHz long GI [bit 22] Data IV:bbc4 Pad 20 KeyID 0
01:02:36.431026 8414442102us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] BA RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.431226 8414442296us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.431245 8414442339us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.431409 5180 MHz 11a -36dBm signal User 0 MCS 6 LDPC FEC 20 MHz long GI [bit 22] Data IV:bbc5 Pad 20 KeyID 0
01:02:36.431415 8414442472us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] BA RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.432591 8414443660us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.432610 8414443703us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.432952 5180 MHz 11a -36dBm signal User 0 MCS 6 LDPC FEC 20 MHz long GI [bit 22] Data IV:bbc6 Pad 20 KeyID 0
01:02:36.432958 8414444015us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] BA RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.433113 8414444183us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.433132 8414444226us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.433477 5180 MHz 11a -36dBm signal User 0 MCS 6 LDPC FEC 20 MHz long GI [bit 22] Data IV:bbc7 Pad 20 KeyID 0
01:02:36.433487 8414444539us tsft 24.0 Mb/s 5180 MHz 11a -69dBm signal [bit 22] BA RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.433684 8414444751us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.433992 8414445048us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.434084 8414445138us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.434338 8414445390us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.434765 8414445821us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.435420 8414446473us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.435993 8414447048us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.436071 8414447141us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.436336 8414447409us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.436631 8414447704us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.437204 8414448288us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.437598 8414448692us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.437717 8414448790us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.437986 8414449059us tsft 24.0 Mb/s 5180 MHz 11a -57dBm signal [bit 22] Request-To-Send TA:a4:b1:c1:91:4c:72 (oui Unknown)
01:02:36.438038 8414449106us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Clear-To-Send RA:a4:b1:c1:91:4c:72 (oui Unknown)
01:02:36.438106 5180 MHz 11a -59dBm signal User 0 MCS 8 LDPC FEC 20 MHz short GI [bit 22] Data IV:89de Pad 20 KeyID 0
01:02:36.438159 8414449223us tsft 24.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Acknowledgment RA:a4:b1:c1:91:4c:72 (oui Unknown)
01:02:36.438509 8414449593us tsft 12.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.438684 8414449754us tsft 6.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.438804 8414449886us tsft 6.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.439003 8414450089us tsft 6.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.439208 8414450266us tsft 6.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.439537 8414450595us tsft 6.0 Mb/s 5180 MHz 11a -36dBm signal [bit 22] Request-To-Send TA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.439576 8414450662us tsft 6.0 Mb/s 5180 MHz 11a -64dBm signal [bit 22] Clear-To-Send RA:0c:9d:92:54:fe:34 (oui Unknown)
01:02:36.439875 5180 MHz 11a -36dBm signal User 0 MCS 0 LDPC FEC 20 MHz long GI [bit 22] Data IV:5206 Pad 20 KeyID 0
01:02:36.439877 5180 MHz 11a -36dBm signal User 0 MCS 0 LDPC FEC 20 MHz long GI [bit 22] Data IV:5207 Pad 20 KeyID 0
```

## TShark Feature Extraction Workflow Diagram



# Feature Description

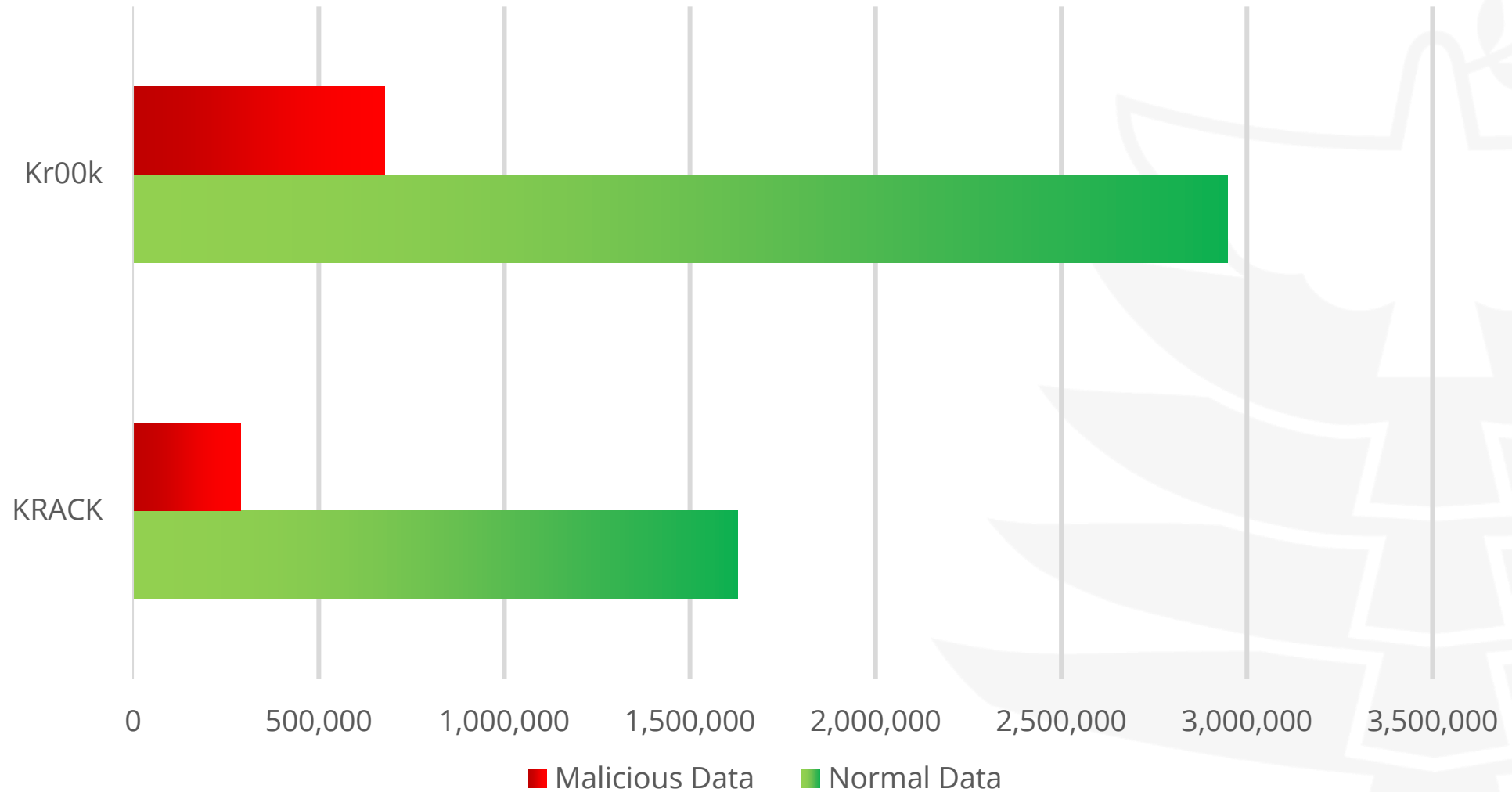


SL No.	Node
1	frame.encap_type
2	frame.len
3	frame.number
4	frame.time
5	frame.time_delta
6	frame.time_delta_displayed
7	frame.time_epoch
8	frame.time_relative
9	radiotap.channel.flags.cck
10	radiotap.channel.flags.ofdm
11	radiotap.channel.freq
12	radiotap.dbm_antsignal
13	radiotap.length
14	radiotap.present.tsft
15	radiotap.rxflags
16	radiotap.timestamp.ts

SL No.	Node
17	wlan.duration
18	wlan.fc.ds
19	wlan.fc.frag
20	wlan.fc.order
21	wlan.fc.moredata
22	wlan.fc.protected
23	wlan.fc.pwrmtgt
24	wlan.fc.type
25	wlan.fc.retry
26	wlan.fc.subtype
27	wlan.ra
28	wlan_radio.duration
29	wlan_radio.channel
30	wlan_radio.data_rate
31	wlan_radio.frequency
32	wlan_radio.signal_dbm

SL No.	Node
33	wlan_radio.phy
34	Label

## Data Characteristics

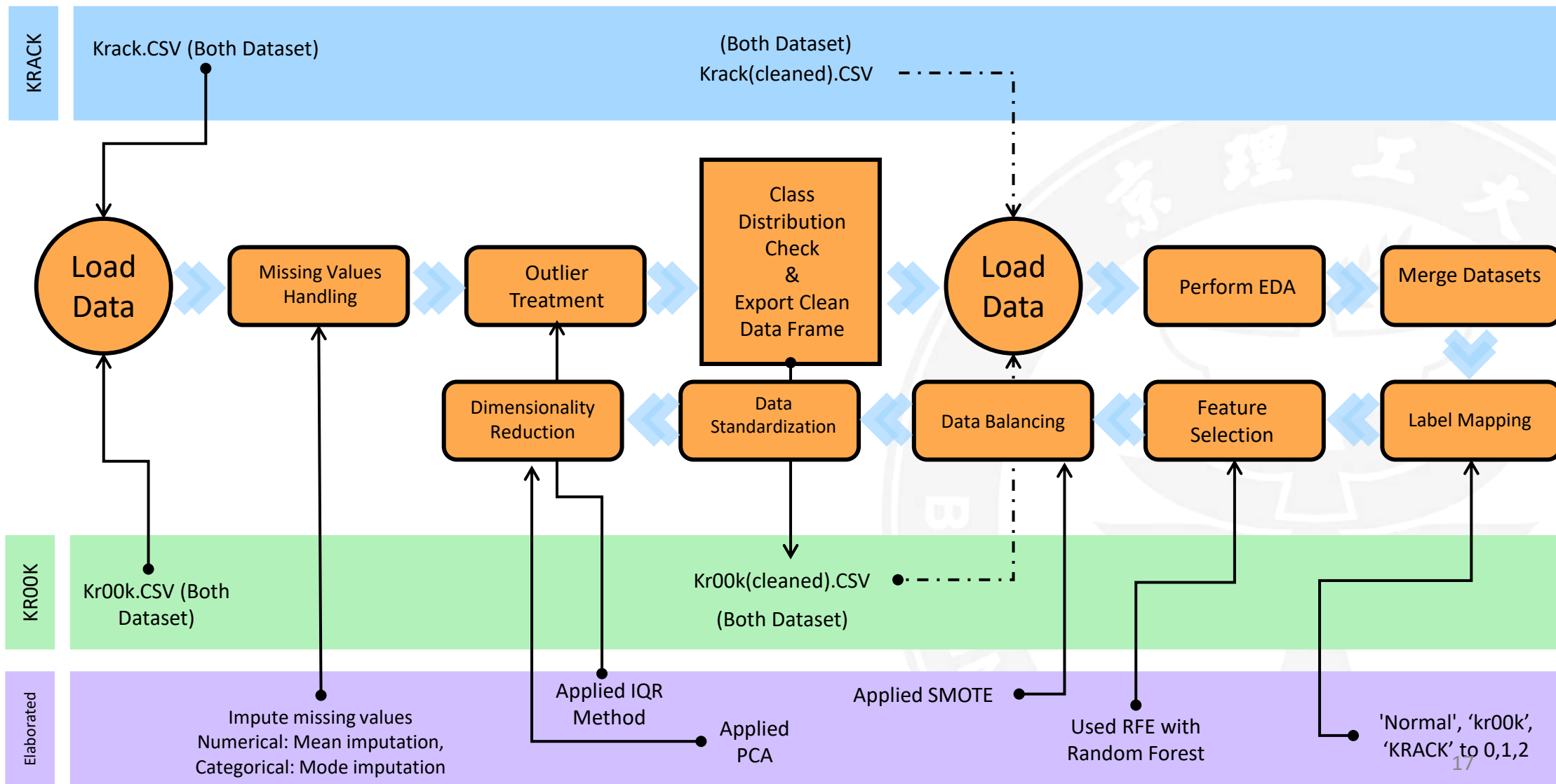


# Model Training & Performance



## Data Preprocessing

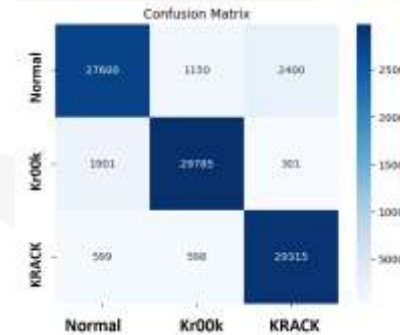
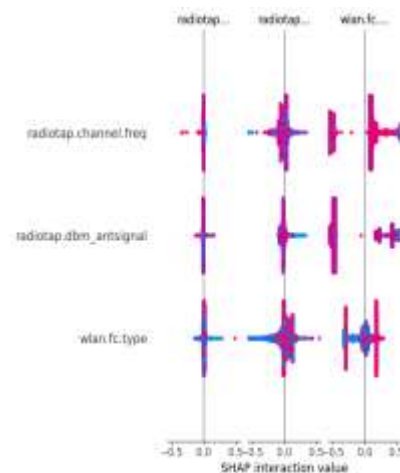
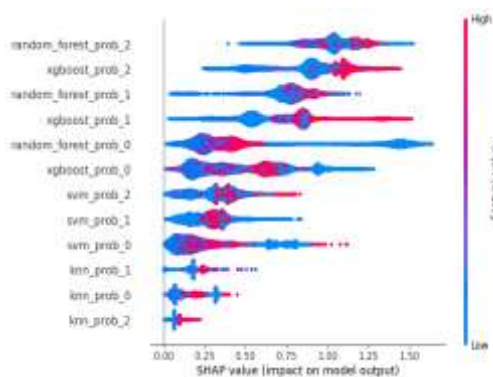
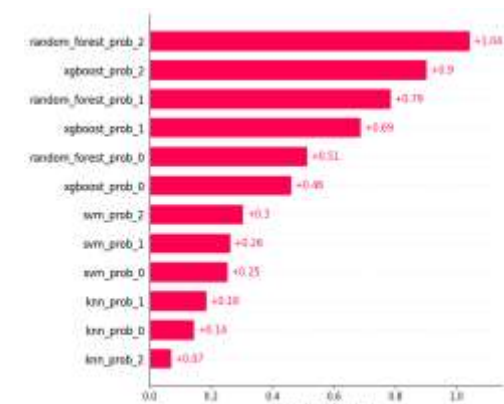
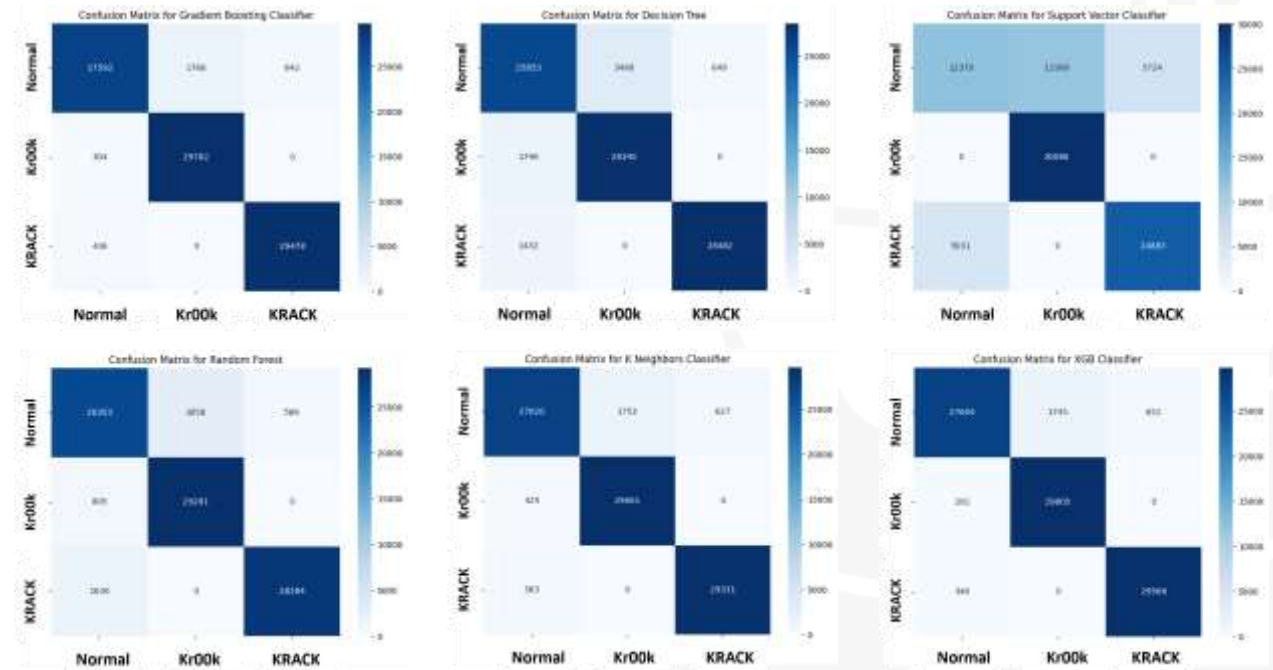
The Foundation of Machine Learning



# Model Training & Performance



Method	Cross-Validation Accuracy	Accuracy	Precision	Recall	F1-Score
Decision Tree	88.76% $\pm$ 0.13	91.86%	91.94%	91.86%	91.86%
Random Forest	92.70% $\pm$ 0.19	93.24%	93.34%	93.24%	93.23%
Support Vector Classifier	76.49% $\pm$ 0.14	74.82%	74.67%	72.64%	72.64%
XGB Classifier	96.48% $\pm$ 0.06	96.64%	96.69%	96.62%	96.62%
Gradient Boosting	96.31% $\pm$ 0.06	96.50%	96.55%	96.48%	96.48%
K Neighbors Classifier	96.17% $\pm$ 0.07	96.24%	96.27%	96.22%	96.22%
Ensemble Method	96.84% $\pm$ 0.26	97.00%	97.02%	97.05%	97.08%







## Expanding Dataset Diversity

Expand the dataset to include Evil Twin and Disassociation attacks, which exploit WPA2 handshake vulnerabilities, and capture data from diverse devices, chipsets, and network configurations to cover a broader range of attack scenarios in varied environments.

## Beyond WPA2

Extend research to WPA3 and other protocols; explore side-channel and application-layer attacks

01

02

03

04

## Improving Model Generalization

Explore advanced techniques for handling class imbalance, such as generative models and data augmentation, while testing the models on real-world network traffic to improve generalization across diverse environments and devices.

## Integration with Network Monitoring Tools

Integrate the expanded dataset into network monitoring tools like Wireshark or Snort for seamless detection of KRACK, Kr00k, Evil Twin, and Disassociation attacks, while exploring cloud-based and distributed systems for scalable intrusion detection across large networks.

知人者智，自知者明。 胜人者有力，自胜者强。 知足者富。 强行者有志。 不失其所者久。 死而不亡者，寿。

## 谢谢！

