802.11 WPA2-Enterprise/EAP/dot1x over-theairワイヤレススニファを復号化するための WiresharkとFreeRADIUSの設定

内容

概要
前提条件
要件
使用するコンポーネント
背景説明
手順
ステップ1:Access-accept PacketからPMKを復号化します。
ステップ2:PMKを抽出します。
ステップ3:OTAスニファを復号化します。
復号化された802.11パケットの例
暗号化された802.11パケットの例
関連情報

概要

このドキュメントでは、Extensible Authentication Protocol(EAP)方式を使用して、Wi-Fi Protected Access 2(WPA2-Enterprise)または802.1x(dot1x)暗号化ワイヤレスover-the-air(OTA)ス ニファを復号化する方法について説明します。

完全な4方向EAP over LAN(EAPoL)ハンドシェイクがキャプチャされている限り、PSKベース /WPA2パーソナル802.11 OTAキャプチャを比較的簡単に復号化できます。ただし、事前共有キー (PSK)は、セキュリティの観点から必ずしも推奨されるわけではありません。ハードコードされ たパスワードを解読するのは時間の問題です。

そのため、多くの企業では、無線ネットワークの優れたセキュリティソリューションとして Remote Authentication Dial-In User Service(RADIUS)を使用してdot1xを選択しています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- radsniffがインストールされたFreeRADIUS
- Wireshark/Omnipeek、または802.11ワイヤレストラフィックを復号化できる任意のソフトウェア
- ネットワークアクセスサーバ(NAS)とオーセンティケーター間の共有秘密を取得する権限を 取得する権限を付与します。

- EAPセッション全体で、最初のアクセス要求(NASからオーセンティケータへ)から最後の アクセス許可(オーセンティケータからNASへ)まで、NASとオーセンティケータ間の RADIUSパケットキャプチャをキャプチャする機能
- •4方向EAPoLハンドシェイクを含むOver-the-Air(OTA)キャプチャを実行する機能

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Radiusサーバ(FreeRADIUSまたはISE)
- Over-the-Airキャプチャデバイス
- Apple macOS/OS XまたはLinuxデバイス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

この例では、2つのペアワイズマスターキー(PMK)は、ISE 2.3からキャプチャされたRADIUSパケットから取得されます。このSSIDのセッションタイムアウトは1800秒で、ここで指定されるキャプチャの長さは34分(2040秒)です。

図に示すように、例としてEAP-PEAPが使用されますが、これは任意のdot1xベースのワイヤレス 認証に適用できます。

	wlan.addr==04:f1:28:6a:69:11 && (eapol or ea	p)		Expression	4
No	o. Time	Source	Destination	Protocol Length Info	Ŀ
Т	4325 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, TLS EAP (EAP-TLS)	L
	4327 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAR 73 Response, Legacy Nak (Response Only)	4
T	4329 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, Protected EAP (EAP-PEAP)	
Т	4332 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	ILSVI.2 244 Client Hello	P
	4349 2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 1079 Server Hello. Certificate. Server Key Exchange. Server Hello	L
T	4352 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	L
T	4354 2018-11-16 00:04:02.833165	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 1075 Server Hello, Certificate, Server Key Exchange, Server Hello	L
	4356 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	L
	4361 2018-11-16 00:04:02.839052	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 738 Server Hello, Certificate, Server Key Exchange, Server Hello	L
	4363 2018-11-16 00:04:02.845892	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 199 Client Key Exchange, Change Cipher Spec, Encrypted Handshake	L
	4365 2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 124 Change Cipher Spec, Encrypted Handshake Message	L
	4367 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	ŀ
1					

	l 🧾 💿 🕌 🔚 🔀 🗳 9, 👄 👄	≝ 7 ± . . Q Q Q . .			+
H MIG	n.addr ==04(11)28(68(69)11 dia (eapoi or eap	y			-
No.	Time	Source	Destination	Protocol Length Info	^
90	95. 2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 754 Encrypted Handshake Message, Encrypted Handshake Message, E	
98	95. 2018-11-16 00:34:07.519109	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 215 Encrypted Handshake Message, Change Cipher Spec, Encrypted I	
90	95. 2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 140 Change Cipher Spec, Encrypted Handshake Message	
90	95. 2018-11-16 00:34:07.525423	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 89 Response, Protected EAP (EAP-PEAP)	
90	95. 2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 125 Application Data	
98	95. 2018-11-16 00:34:07.529567	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 129 Application Data	
98	95. 2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 151 Application Data	
90	95_ 2018-11-16 00:34:07.536570	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 183 Application Data	
90	95_ 2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 169 Application Data	
90	95. 2018-11-16 00:34:07.570964	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 124 Application Data	-
98	95_ 2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 125 Application Data	
98	95_ 2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 89 Response, Protected EAP (EAP-PEAP)	~

手順

ステップ1:Access-accept PacketからPMKを復号化します。

PMKを抽出するには、NASとオーセンティケータ間のRADIUSキャプチャに対してradsniffを実行 します。キャプチャ中に2つのaccess-acceptパケットが抽出される理由は、この特定のSSIDでセ ッションタイムアウトタイマーが30分に設定され、キャプチャの長さが34分であることです。認

証は2回実行されます。

```
FRLU-M-51X5:pcaps frlu$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -
s <shared-secret between NAS and Authenticator> -x
<snip>
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a306134323466326130303030303565373562656530393732
Class =
2f33303432
EAP-Message = 0x03c50004
Message-Authenticator = 0x38c67b9ba349842c9624889a45cabdfb
MS-MPPE-Send-Key = 0xa464cc15c0df8f09edc249c28711eb13a6db2d1a176f1196edcc707579fd6793
MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b<<<<<<<<<PMK
Authenticator-Field = 0x6cd33b4d4dde05c07d9923e17ad6c218
<snip>
2018-11-16 11:39:01.470000 (48) Access-Accept Id 183
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
0x434143533a3061343234663261303030303035653735626565303937323a4953452d322d332f333238323731323338
2f33303434
EAP-Message = 0x03910004
Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9
MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb
MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e<<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
    注:Radiusパケットキャプチャの仮想LAN(VLAN)タグを削除してください。削除しない場
    合、radsniffは入力pcapファイルを認識しません。VLANタグを削除するには、たとえば
```

editcapを使用できます。

ヒント:通常、RADIUS pcapファイルに対するradsniffコマンドの実行時は、秒のスケール

としてカウントできます。ただし、ログに示されたこの状態で**radsniffがスタックしている** 場合は、同じNASとオーセンティケータの間で別の長いパケットキャプチャ(B)を使用して 、このパケットキャプチャ(A)をカスケードしてください。次に、カスケードされたパケッ ト(A+B)に対してradsniffコマンドを実行します。 パケットキャプチャ(B)の唯一の要件は、 radsniffコマンドを実行して詳細な結果を表示できることです。

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Cisco123 -x

Logging all events

Sniffing on (/Users/frlu/Downloads/radius_novlan.pcap)

この例では、WLCパケットロギング機能によってキャプチャされたワイヤレスLANコントローラ (WLC)コントロールプレーンロギング(A)が、ISEのTCPダンプ(B)からより長いキャプチャにカス ケードされています。WLCパケットロギングは通常、非常に小さいサイズであるため、例として 使用されます。

WLCパケットロギング(A)

📅 radius_novlan.pcap	Pcap Napture	22 KB	Today at 11:56 am	
ISE Tcpdump(B)				
radius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm		850 KB Pcap Nap	ture
マージ(A+B)				
🚡 radius_novlan_merged.pcapng	PcapnCapture	927 KB	Today at 12:28 pm	

次に、マージされたpcap(A+B)に対してradsniffを実行すると、詳細な出力が表示されます。

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -s
<shared-secret between NAS and Authenticator> -x

<snip>

2018-11-16 11:39:01.230000 (24) Access-Accept Id 172 /Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000 +0.000

<snip>

ステップ2:PMKを抽出します。

その後、詳細出力から各**MS-MPPE-Recv-Keyの0xフィールドを削除**し、ワイヤレストラフィック デコードに必要なPMKを提示します。

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

PMK: ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e PMK: 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

ステップ3:OTAスニファを復号化します。

[Wireshark] > [Preferences] > [Protocols] > [IEEE 802.11]に移動し、[Enable Decryption]をオンに し、[Decryption Keys]の横にある[Edit]ボタンをクリックします。

4	Wireshark · Preferences	?	x
HCrt ADFSDATA HDFSDATA HIP HGnet HISLIP HIC7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 IAPP IAX2 IB ICAP ICP ICP ICP ICQ IEEE 802.11 IEEE 802.15.4 ~	If B02.11 wireless LAN Ignore vendor-specific HT elements Ignore vendor-specific HT elements Call subdissector for retransmitted 802.11 frames Assume packets have FCS Validate the FCS checksum if possible Ignore the Protection bit No Yes - without IV Yes - with IV WPA Key MDC Length override Decryption keys Edit	Help	9

次に、キーの種類として**wpa-pskを選**択し、[Key]フィールドに導出されたPMKを入力し、[**OK**]を クリックし**てください**。これが完了すると、OTAキャプチャが復号化され、上位レイヤ(3+)情報 が表示されます。

	Wireshark - Preferences ?	×
	WEP and WPA Decryption Keys	
	Key type Key wpa-psk ddb0b09a7d6980515825950b5929d02/236799f3e8a87f163c8ca41a066d8b3b wpa-psk 7ccce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e	
<	+ - D A V R Cancel Help	

復号化された802.11パケットの例

File Edit	View Go Capture Analyze Statistics	Telephony Wireless Tools Help			
	🖲 📙 🗅 🗙 🗖 🍳 👄 🕾 🖗 🕸	🔲 🔳 @, @, @, II			
wlan.add	r==04:f1:28:6a:69:11				🛛 🔜 💌 Expression +
No.	Time	Source	Destination	Protocol	Length Info
1	397877 2018-11-16 00:17:08.095884	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45 Request-to-send, Flags=C
	397879 2018-11-16 00:17:08.097877	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45 Request-to-send, Flags=C
	397881 2018-11-16 00:17:08.098393	40.127.66.24	172.16.255.13	TCP	1438 [TCP Retransmission] 80 → 45658 [ACK] Seq=3999908
	397882 2018-11-16 00:17:08.098444	104.17.57.239	172.16.255.13	TCP	154 80 → 37553 [ACK] Seq=1 Ack=310 Win=65344 Len=0 TS
	397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57 802.11 Block Ack, Flags=C
	397884 2018-11-16 00:17:08.098999	104.17.57.239	172.16.255.13	TCP	162 80 → 37555 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
	397886 2018-11-16 00:17:08.099099	172.16.255.13	40.127.66.24	TCP	154 45658 → 80 [ACK] Seq=128 Ack=4001196 Win=788480 L
	397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (1_	HmdGloba_6a:69:11 (04:11:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=
	397888 2018-11-16 00:17:08.099606	172.16.255.13	104.17.57.239	TCP	154 37555 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSva
	397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
	397890 2018-11-16 00:17:08.101762	172.16.255.13	104.17.57.239	HTTP	479 GET /s100264/images/logoq.png?t=636366 HTTP/1.1
1	397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
<					>
Frame	397886: 154 bytes on wire (1232 bits),	, 154 bytes captured (1232 bits)			
Radiot	ap Header v0, Length 48				
▶ 802.11	radio information				
IEEE 8	02.11 QoS Data, Flags: .pTC				
Logica	1-Link Control				
Intern	et Protocol Version 4, Src: 172.16.255	5.13, Dst: 40.127.66.24			
Transm	ission Control Protocol, Src Port: 456	558, Dst Port: 80, Seq: 128, Ack: 4001196	, Len: 0		
0000 00	00 30 00 6b 08 1c 00 6d f9 30 31 00	00 00 00 ···0·k··· m·01····			
0010 14	00 9e 09 80 04 d9 a4 00 00 00 80	04 01 00			
0020 9e	09 0b 22 1f 00 06 00 65 00 00 00 04	00 00 00 ····"···· e·····			
0030 88	41 30 00 00 a3 8e b4 3d e4 04 f1 28	6a 69 11 · A0· · · · (ji·			
0040 00	0c 29 28 89 dd 50 06 00 00 c8 84 00	20 01 00 ···)(··P······			
0050 00	00 at t4 c2 2t 90 d1 14 52 a5 80 2e	5/ 2/ 3a/····R···W·:			
0070 50	98 7a 36 57 cd e2 43 89 86 f5 92 24	17 d0 db \.z6W-C\$			
0080 42	a2 2e 62 35 c7 36 9b 54 d0 00 91 78	7d 44 87 B b5.6. T x}D.			
0090 23	6c 7b e6 fd db e7 06 39 11	#1{9.			

PMKが含まれていない2番目の結果と、PMKが含まれている1番目の結果を比較すると、パケット 397886は802.11 QoSデータとして復号化されます。

暗号化された802.11パケットの例

Time Source Destination Protocil Length Info 397881 2018-11-16 00:17:08.098344 Wmare_28:09:dd HindGloba_6a:69:11 0802.11 1438 Gos Data, Sh=1434, File®, Flags=.pF,C 397882 2018-11-16 00:17:08.098445 Wmare_28:09:idd HindGloba_6a:69:11 0802.11 154 QS Data, Sh=4335, File®, Flags=.pF,C 397883 2018-11-16 00:17:08.098445 Wmare_28:09:idd HindGloba_6a:69:11 0802.11 57 802.11 Block Ack, Flags=.pFC 397884 2018-11-16 00:17:08.099999 HindGloba_6a:69:11 Wmare_28:09:idd 802.11 57 802.11 154 QS Data, Sh=1434, File®, Flags=.p,FC 397884 2018-11-16 00:17:08.099999 HindGloba_6a:69:11 Wmare_28:09:idd 802.11 154 QS Data, Sh=1434, File®, Flags=.p,TC 397885 2018-11-16 00:17:08.099956 HindGloba_6a:69:11 Wmare_28:09:idd 802.11 154 QS Data, Sh=1434, File®, Flags=.p,TC 397889 2018-116 00:17:08.099656 HindGloba_6a:69:11 (Mirf 1:28:6a:69:11)	vlan.ac	dr==04:f1:28:6a:69:11					Expre
397881 2018-11-16 00:17:08.098434 Vmmare_28:99:dd HmdGloba_68:69:11 802.11 1438 QoS Data, Sh=1435, FH=0, Flags=.pF, C 397882 2018-11-16 00:17:08.098444 Vmmare_28:89:dd HmdGloba_68:69:11 802.11 154 QoS Data, Sh=1435, FH=0, Flags=.pF, C 397883 2018-11-16 00:17:08.098449 Vmmare_28:89:dd HmdGloba_68:69:11 802.11 154 QoS Data, Sh=1435, FH=0, Flags=.p,F, C 397884 2018-11-16 00:17:08.099099 HmdGloba_68:69:11 Vmmare_28:89:dd 802.11 154 QoS Data, Sh=1435, FH=0, Flags=.p,F, C 397885 2018-11-16 00:17:08.099099 HmdGloba_68:69:11 Vmmare_28:89:dd 802.11 154 QoS Data, Sh=10, FH=0, Flags=.p,TC 397885 2018-11-16 00:17:08.099099 HmdGloba_68:69:11 Vmmare_28:89:dd 802.11 154 QoS Data, Sh=02, FH=0, Flags=.p,TC 397885 2018-11-16 00:17:08.099050 Cisco_b4:34:e4 (00:a3:8e:b4:3d:e4) (T_H HmdGloba_68:69:11 (04:f1:28:68:69:11) (RA) 802.11 154 QoS Data, Sh=02, FH=0, Flags=.p,TC 397892 2018-11-16 00:17:08.01762 HmdGloba_68:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=04, Flags=.p,TC 397892 2018-11-16 00:17:08.01762 HmdGloba_68:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=04, Flags=.p,TC 397892 2018-11-16 00:17:08.019055 Wmware_28:89:dd		Time	Source	Destination	Protocol	Length Info	
397862 2018-11-16 00:17:08.098495 Vmaare_28:09:dd HedGloba_6a:69:11 802.11 154 QOS Data, SN=1435, FH=0; Flags-,p,F.C 397863 2018-11-16 00:17:08.098495 HedGloba_6a:69:11 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (RA) 802.11 154 QOS Data, SN=1435, FH=0; Flags-,p,F.C 397864 2018-11-16 00:17:08.098495 Vmaare_28:89:dd HedGloba_6a:69:11 802.11 154 QOS Data, SN=1435, FH=0; Flags-,p,FC 397865 2018-11-16 00:17:08.099895 HedGloba_6a:69:11 Vmaare_28:89:dd 802.11 154 QOS Data, SN=1435, FH=0; Flags-,p,TC 397867 2018-11-16 00:17:08.099855 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (T- HedGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QOS Data, SN=1435, FH=0; Flags-,p,TC 397868 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (T- HedGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QOS Data, SN=143, FH=0; Flags-,p,TC 397869 2018-11-16 00:17:08.101722 HedGloba_6a:69:11 Wmare_28:89:dd 802.11 158 QOS Data, SN=1437, FH=0; Flags-,p,TC 397892 2018-11-16 00:17:08.101722 HedGloba_6a:69:11 Wmare_28:89:dd 802.11 558 QOS Data, SN=1437, FH=0; Flags-,p,F.C 397892 2018-11-16 00:17:08.10172 Cisco_b4:3d:e4 (00:a3:8e:14:3d:e4) (T- HedGloba_6a:69:11] 802.11 558 QOS Data, S		397881 2018-11-16 00:17:08.098393	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	1438 QoS Data, SN=1434, FN=0, Flags=.pR.F.C	
397883 2018-11-16 00:17:08.098999 HmdGloba_6a:69:11 (0:f1:28:6a:69:11) - Clsco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA) 802.11 57 802.111 Block Ack, Flags=C 397884 2018-11-16 00:17:08.098999 Vmware_28:89:d4 802.11 802.11 152 Qo5 Data, SN-1436, FH-0, Flags=.p,C 397885 2018-11-16 00:17:08.099998 MmdGloba_6a:69:11 Vmware_28:89:d4 802.11 154 Qo5 Data, SN-1436, FH-0, Flags=.p,TC 397885 2018-11-16 00:17:08.099958 Clsco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) Vmware_28:89:d4 802.11 154 Qo5 Data, SN-1436, FH-0, Flags=.p,TC 397885 2018-11-16 00:17:08.099658 Clsco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (RA) 802.11 154 Qo5 Data, SN-108, FH-0, Flags=.p,TC 397895 2018-11-16 00:17:08.101702 Lisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (RA) 802.11 154 Qo5 Data, SN-103, FH-0, Flags=.p,TC 397895 2018-11-16 00:17:08.101702 HmdGloba_6a:69:11 Vmware_28:89:d4 802.11 155 Qo5 Data, SN-103, FH-0, Flags=.p,TC 397895 2018-11-16 00:17:08.101702 HmdGloba_6a:69:11 Vmware_28:89:d4 802.11 155 Qo5 Data, SN-143, FH-0, Flags=.p,TC 397892 2018-11-16 00:17:08.105055 Vmware_28:89:d4 HmdGloba_6a:69:11 802.11 595 Qo5 Data, SN-1437, FH-0, Flags=.p,FC 397892 2018-1		397882 2018-11-16 00:17:08.098444	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1435, FN=0, Flags=.pF.C	
39784 2018-11-16 00:17:08.099999 Vmare_28:09:dd Hediloba_6a:69:11 Vmare 28:09:dd 602.11 154 Qo5 Data, SN=101, FN=0, Flagspf.C 397868 2018-11-16 00:17:08.099999 Hediloba_6a:69:11 Vmare 28:09:dd 602.11 154 Qo5 Data, SN=101, FN=0, FlagspTC 397867 2018-11-16 00:17:08.099909 Hediloba_6a:09:11 (Gu f1:28:66:09:11) (RA) 602.11 154 Qo5 Data, SN=102, FN=0, FlagspTC 397867 2018-11-16 00:17:08.099505 Cisco_41:3d:e4 (G0:a3:08:14:3d:e4) (T.= Hediloba_6a:09:11) (Gu f1:28:66:09:11) (RA) 602.11 154 Qo5 Data, SN=102, FN=0, FlagspTC 397867 2018-11-16 00:17:08.009555 Cisco_41:3d:e4 (G0:a3:08:14:44: (U = Midiloba_6a:09:11) (Gu f1:28:66:09:11) (RA) 602.11 155 Qo5 Data, SN=108, FlagspTC 397869 2018-11-16 00:17:08.009555 Vmare_22:89:dd Hediloba_6a:09:11 (Gu f1:28:66:09:11) (RA) 602.11 57 Go2.11 Block Ack, FlagspTC 397892 2018-11-16 00:17:08.101812 Cisco_41:3d:e4 (00:a3:8e:14:3d:e4) (T.= Hediloba_6a:69:11) (Gu f1:28:6a:69:11) (RA) 602.11 57 Go2.11 Block Ack, Flagsp,FC 397892 2018-11-16 00:17:08.105555 Vmare 28:89:dd Hediloba_6a:69:11 602.11 59 Qo5 Data, SN=1437, FN=0, Flagsp,FC 397894 2018-11-16 00:17:08.105555 Vmare 28:89:dd Hediloba_6a:69:11 602.11 502 Data, SN=1433, FN=0, Flagsp,FC		397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397865 2018-11-16 00:17:08.09909 HmdGloba_6a:69:11 Vmmare 28:89:dd 802.11 154 Qo5 Data, SN-181, FN-0, Flags-,TC 397867 2018-11-16 00:17:08.099181 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) Vmmare 28:89:dd 802.11 154 Qo5 Data, SN-182, FN-0, Flags-,TC 397868 2018-11-16 00:17:08.09966 HmdGloba_6a:69:11 Vmmare 28:89:dd 802.11 154 Qo5 Data, SN-182, FN-0, Flags-,TC 397869 2018-11-16 00:17:08.099665 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11) (RA) 802.11 155 QO5 Data, SN-183, FN-0, Flags-,TC 397892 2018-11-16 00:17:08.101622 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags-,C 397892 2018-11-16 00:17:08.101622 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags-,C 397892 2018-11-16 00:17:08.106055 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 58 QO2.11 Block Ack, Flags-,, C 397894 2018-11-16 00:17:08.106056 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 58 QO2.11 Block Ack, Flags-,, C 397894 2018-11-16 00:17:08.106056 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 58 QO2.11 Block Ack, Flags-,, F.C S80.211 S80		397884 2018-11-16 00:17:08.098999	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	162 QoS Data, SN-1436, FN-0, FlagspF.C	_
397867 2018-11-16 00:17:08.099168 Cisco_b4:3:de:4 (00:a3:8e:b4:3d:e4) (T. HedGloba_6a:69:11) (RA) 802.11 57 802.11 block Ack; Plags*C 397868 2018-11-16 00:17:08.09965 Cisco_b4:3:de:4 (00:a3:8e:b4:3d:e4) (T. HedGloba_6a:69:11) (RA) 802.11 154 005 Data, SN=102, FN=0,		397886 2018-11-16 00:17:08.099099	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=101, FN=0, Flags=.pTC	
397888 2018-11-16 00:17:08.099565 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 154 QoS Data, SN=102, FH-08, Flags=, pTC 397898 2018-11-16 00:17:08.101762 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 154 QoS Data, SN=103, FH-08, Flags=, pTC 397899 2018-11-16 00:17:08.101762 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 57 802.111 57 802.11 Block Ack, Flags=, pTC 397891 2018-11-16 00:17:08.101762 Lisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T- HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, pTC 397892 2018-11-16 00:17:08.10182 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T- HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, pTC 397892 2018-11-16 00:17:08.10182 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T- HmdGloba_6a:69:11 (RA) 802.11 59 QoS Data, SN=103, FN=0, Flags=, pTC 397894 2018-11-16 00:17:08.10182 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T- HmdGloba_6a:69:11 (RA) 802.11 59 QoS Data, SN=143, FN=0, Flags=, pTC 397894 2018-11-16 00:17:08.106555 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 54 QoS Data, SN=1438, FN=0, Flags=, pFC Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Is4 QoS Data, Flags: pFC S8 QoS Data, SN=1438, FN=0, Flags=, pFC Bo2.111 QoS Data, Flags: pTC Data (68 bytes)		397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=	_
397869 2018-11-16 00:17:08.099655 Cisco_b4:3:d:e4 (00:a3:8e:b4:3d:e4) (T_ HedGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 397809 2018-11-16 00:17:08.101762 HedGloba_6a:69:11 Umware_28:89:dd 802.11 479 QoS Data, SN=103, FN=0,		397888 2018-11-16 00:17:08.099606	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=102, FN=0, Flags=.pTC	
397890 2018-11-16 00:17:08.101762 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 479 QoS Data, SN=103, FH=0, Flags=.pTC 397892 2018-11-16 00:17:08.101312 Cicco_b43:dete(00:03:88:b4:43:det) (T= HmdGloba_6a:69:11) 802.11 578 QoS Data, SN=1043, FH=0, Flags=.pFC 397892 2018-11-16 00:17:08.105058 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 559 QoS Data, SN=1437, FH=0, Flags=.pFC 397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 559 QoS Data, SN=1437, FH=0, Flags=.pFC Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 B02.11 QoS Data, Flags: .pTC Data (68 bytes)		397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397891 2018-11-16 00:17:08.101012 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.105958 Vmware_28:89:dd HmdGloba_6a:69:11) 802.11 555 QoS Data, SN=1437, FN=0, Flags=.pF.C 397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1437, FN=0, Flags=.pF.C 9978964 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1437, FN=0, Flags=.pF.C 9978965: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes captured (1232 bits) 154 Redictap Header v0, Length 48 802.11 QoS Data, Flags: .pTC Data (68 bytes) Flags: .pTC		397890 2018-11-16 00:17:08.101762	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	479 QoS Data, SN=103, FN=0, Flags=.pTC	
397892 2018-11-16 00:17:08.105955 Vmware_28:89:dd HmdGloba_6a:69:11 602.11 509 CoS Data, SN=1437, FN+0, FlagspF.C 397892 2018-11-16 00:17:08.105056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, FlagspF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 154 CoS Data, Flags: .pF.C B02.11 QOS Data, Flags: .pTC Data (68 bytes) Image: .pTC Image: .pTC		397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397894 2018-11-16 00:17:08.106055 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, Flags*.pF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Bits) Interview of the second		397892 2018-11-16 00:17:08.105958	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	595 QoS Data, SN=1437, FN=0, Flags=.pF.C	
Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Data (68 bytes)		397894 2018-11-16 00:17:08.106056	Vmware 28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1438, FN=0, Flags=.pF.C	
	Frame Radio 802.1 IEEE Data	397865: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes)	154 bytes captured (1232 bits)				
	Frame Radio 802.1 IEEE Data	39786: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes)	154 bytes captured (1232 bits)				
00 00 60 30 00 60 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <td< td=""><td>Frame Radio 802.1 IEEE Data</td><td>39786: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes)</td><td>154 bytes captured (1232 bits)</td><td></td><td></td><td></td><td></td></td<>	Frame Radio 802.1 IEEE Data	39786: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes)	154 bytes captured (1232 bits)				
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <td< td=""><td>Frame Radio 802.1 IEEE Data Data 000 00 010 1 020 9 030 8 030 8</td><td>39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 00 9c 09 30 04 d9 a4 00 00 00 80 0 90 9b 22 1f 00 06 00 65 20 00 00 4 41 30 00 00 a3 8b b4 3d e4 04 f1 28 0c c29 28 3d d5 06 00 e0 ce 8 6 48 28</td><td>154 bytes captured (1232 bits)</td><td></td><td></td><td></td><td></td></td<>	Frame Radio 802.1 IEEE Data Data 000 00 010 1 020 9 030 8 030 8	39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 00 9c 09 30 04 d9 a4 00 00 00 80 0 90 9b 22 1f 00 06 00 65 20 00 00 4 41 30 00 00 a3 8b b4 3d e4 04 f1 28 0c c29 28 3d d5 06 00 e0 ce 8 6 48 28	154 bytes captured (1232 bits)				
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <td< td=""><td>Frame Radio 802.1 IEEE Data Data 000 00 010 10 020 9 030 00 0340 00 0350 00</td><td>39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 00 9e 09 80 04 d9 a4 00 9e 09 80 04 d9 a4 14 13 00 00 00 38 0e 54 36 e4 04 f1 28 0c 29 28 89 d4 59 06 00 00 c8 84 00 00 06 ff 42 22 f9 04 11 452 a5 8b 2e</td><td>154 bytes captured (1232 bits)</td><td></td><td></td><td></td><td></td></td<>	Frame Radio 802.1 IEEE Data Data 000 00 010 10 020 9 030 00 0340 00 0350 00	39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 00 9e 09 80 04 d9 a4 00 9e 09 80 04 d9 a4 14 13 00 00 00 38 0e 54 36 e4 04 f1 28 0c 29 28 89 d4 59 06 00 00 c8 84 00 00 06 ff 42 22 f9 04 11 452 a5 8b 2e	154 bytes captured (1232 bits)				
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <td< td=""><td>Frame Radio 802.1 IEEE Data Data 000 00 010 10 020 90 030 80 040 00 050 00 0650 00 0650 00</td><td>397886: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 102.11 QoS Data, Flags: .pTC (68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 09 09 22 1f 00 06 00 65 00 00 08 09 0b 22 1f 00 06 00 65 00 00 00 84 09 0b 22 1f 00 06 00 65 00 00 08 41 30 00 00 a3 06 b4 33 46 44 12 0 c 29 28 39 d5 30 60 00 06 84 00 100 27 42 27 90 d1 14 52 a5 bb 2 0 48 54 35 50 12 92 da fa 91 fa 2 c 8</td><td>154 bytes captured (1232 bits)</td><td></td><td></td><td></td><td></td></td<>	Frame Radio 802.1 IEEE Data Data 000 00 010 10 020 90 030 80 040 00 050 00 0650 00 0650 00	397886: 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 102.11 QoS Data, Flags: .pTC (68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 09 09 22 1f 00 06 00 65 00 00 08 09 0b 22 1f 00 06 00 65 00 00 00 84 09 0b 22 1f 00 06 00 65 00 00 08 41 30 00 00 a3 06 b4 33 46 44 12 0 c 29 28 39 d5 30 60 00 06 84 00 100 27 42 27 90 d1 14 52 a5 bb 2 0 48 54 35 50 12 92 da fa 91 fa 2 c 8	154 bytes captured (1232 bits)				
800 60 60 60 61 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 <t< td=""><td>Frame Radio 802.1 IEEE Data 000 00 010 10 020 90 030 80 040 00 050 00 00 050 00 050 00 00000000</td><td>39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 000 30 00 6b 08 1c 00 6d f9 30 31 00 000 9e 09 30 04 d9 a4 00 00 00 80 09 0b 22 1f 00 06 00 65 00 00 00 00 4 13 30 00 00 a3 06 54 00 00 09 f4 c2 2f 90 d1 14 52 a5 8b 2e 54 a5 55 0a 12 92 da fc a9 1f c2 c8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 58 7a 65 7c de 24 3 80 66 f5 92 24</td><td>154 bytes captured (1232 bits) 00 00 000.k. m.01</td><td></td><td></td><td></td><td></td></t<>	Frame Radio 802.1 IEEE Data 000 00 010 10 020 90 030 80 040 00 050 00 00 050 00 050 00 00000000	39786; 154 bytes on wire (1232 bits), tap Header v0, Length 48 radio information 302.11 QoS Data, Flags: .pTC (68 bytes) 000 30 00 6b 08 1c 00 6d f9 30 31 00 000 9e 09 30 04 d9 a4 00 00 00 80 09 0b 22 1f 00 06 00 65 00 00 00 00 4 13 30 00 00 a3 06 54 00 00 09 f4 c2 2f 90 d1 14 52 a5 8b 2e 54 a5 55 0a 12 92 da fc a9 1f c2 c8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 58 7a 65 7c de 24 3 80 66 f5 92 24	154 bytes captured (1232 bits) 00 00 000.k. m.01				

注意:復号化時にWiresharkで問題が発生する可能性があり、その場合は、正しいPMKが指定されている(またはPSKが使用されている場合は、SSIDとPSKの両方が指定されている)場合でも、WiresharkはOTAキャプチャを復号化しません。この問題を回避するには、Wiresharkの電源をオフにしてから、上位レイヤ情報を取得して802.11パケットがQoSデータとして表示されなくなるまで数回使用するか、Wiresharkがインストールされている別のPC/Macを使用します。

ヒント: pmkXtractというC++コードが関連情報の最初の投稿に添付されています。コンパイ ルが正常に行われ、実行可能ファイルが取得されましたが、実行可能プログラムが正常に復 号化を行っていないことが判明した理由があります。また、PMKを抽出しようとする Pythonスクリプトは、最初の投稿のコメント領域に投稿されます。このコメント領域は、 読者が興味を持っている場合に詳しく調べることができます。

関連情報

- EAPの弱いリンクの調整 pmkXtractを使用したWiFi PMKのRADIUSからの吸引
- RADIUS MS-MPPE-Recv-Keyのデコード方法
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>