Wireless-shark en FreeRADIUS configureren voor het decrypteren van 802.11 WAP2-Enterprise/EAP/dot1x-luchtdraadloze snelkiezer

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Procedure Stap 1. Versleutel PMK(s) van access-accepteer Packet. Stap 2: PMK(en) uittrekken. Stap 3. Ontdek de OTA-slang. Voorbeeld van een gedecrypteerd 802.11 Packet Voorbeeld van een versleuteld 802.11 Packet Gerelateerde informatie

Inleiding

In dit document wordt beschreven hoe u Wi-Fi beschermde access 2 - Enterprise (WAP2-Enterprise) of 802.1x (dot1x) versleutelde Wireless-over-the-air (OTA) snuifje kunt decrypteren, met alle MAP-methoden (Extensible Verification Protocol).

Het is relatief gemakkelijk om op PSK gebaseerde/WAP2-persoonlijke 802.11 OTA-opname te decrypteren zolang de volledige viervoudige EAP over LAN (EAPoL)-handleidingen worden opgenomen. Vooraf gedeelde sleutel (PSK) wordt echter niet altijd vanuit veiligheidsoogpunt aanbevolen. Het is een kwestie van tijd om een hard gecodeerd wachtwoord in te trekken.

Vandaar dat veel ondernemingen kiezen voor dot1x met afstandsverificatie Dial-In User Service (RADIUS) als een betere beveiligingsoplossing voor hun draadloze netwerk.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FreeRADIUS met radsniff geïnstalleerd
- Wireshark/Omnipeek of alle software die 802.11 draadloos verkeer kan decrypteren
- Bevoegd om het gedeelde geheim tussen netwerk access server (NAS) en Authenticator te verkrijgen
- Mogelijkheid om Straal pakketvastlegging tussen NAS en authenticator op te nemen van het

eerste toegangsverzoek (van NAS tot Authenticator) tot het laatste toegangsaanvaarden (van Authenticator tot NAS) gedurende de MAP-sessie

 Mogelijkheid om OTA-opname (over-the-Air) uit te voeren die viervoudige EAPoLhandschoenen bevat

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Radius-server (FreeRADIUS of ISE)
- Luchtvanger
- Apple Max/OS/X of Linux-apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In dit voorbeeld worden twee Pairwise Master Keys (PMKs) afgeleid van Radius-pakketten die zijn opgenomen van ISE 2.3, omdat de sessietijd op deze SSID 1800 seconden is en de hier gegeven opname 34 minuten (2040 seconden) lang is.

Zoals in de afbeelding wordt getoond, wordt EAP-PEAP als voorbeeld gebruikt, maar dit kan worden toegepast op elke op dot1x gebaseerde draadloze authenticatie.

]	wlan.a	ddr==04:f1:28:6a:69:11 && (eapol or eap)		Expression	4
N	o.	Time	Source	Destination	Protocol Length Info	P
	432	5 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, TLS EAP (EAP-TLS)	L
	432	7 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Legacy Nak (Response Only)	Ł
	432	9 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, Protected EAP (EAP-PEAP)	1
	433	2 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	ILSVI.2 244 Client Hello	F
	434	9 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
	435	2 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	L
	4354	4 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
	435	6 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	L
	436	1 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
	436	3 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 Handshak	L
	436	5 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
	436	7 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	ŀ
1						

41	i d 🖲 🎴 🗅 🗙 🖨 🍳 👄 👄	se 7 & 🚍 🗏 Q Q Q II				
wi wi	n.addr==04:f1:28:6a:69:11 && (eapol or eap)				🛛 📼 💌 Expression.	+
No.	Time	Source	Destination	Protocol	Length Info	^
99	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, En	
96	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	
96	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	
96	95. 2018-11-16 00:34:07.525423	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)	
96	95 2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	125 Application Data	
99	95. 2018-11-16 00:34:07.529567	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	129 Application Data	
96	95. 2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	151 Application Data	
96	95. 2018-11-16 00:34:07.536570	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	183 Application Data	
96	95. 2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	169 Application Data	
96	95. 2018-11-16 00:34:07.570964	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	124 Application Data	_
90	95_ 2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	125 Application Data	
96	95_ 2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)	~

Procedure

Stap 1. Versleutel PMK(s) van access-accepteer Packet.

Draai de **radsniff** tegen Straalopname tussen NAS en Authenticator om PMK te extraheren. De reden waarom twee pakketten voor toegangscontrole tijdens de opname worden geëxtraheerd is dat de timer voor de sessie op deze specifieke SSID is ingesteld op 30 minuten en de opname 34

minuten lang is. Verificatie wordt tweemaal uitgevoerd.

```
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 =
2f33303434
EAP-Message = 0x03910004
Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9
MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb
MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfblcfb0e<<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

Opmerking: Verwijder een VLAN-tag (VLAN) van de pakketvastlegging door Radius **anders** herkent **Radius** het ingangspenpenbestand niet. Om een VLAN-tag te verwijderen, kan bijvoorbeeld <u>bewerkingsdop</u> worden gebruikt.

Tip: Over het algemeen kan de opdracht van radsniff tegen een RADIUS-penbestand als

een schaal van seconden worden geteld. Als de raster echter vast zit in deze toestand die in het logbestand wordt weergegeven, noteert u deze pakketvastlegging (A) met een andere langere pakketvastlegging (B) tussen dezelfde NAS en Authenticator. Start vervolgens de radiofrequentie tegen het gecasceerde pakje (A+B). Het enige vereiste van pakketvastlegging (B) is dat u de radiofunctie ertegen kunt uitvoeren en breedtegraden resultaat kunt zien.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Ciscol23 -x

Logging all events

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

In dit voorbeeld wordt de controle-plane logging (WLC) van de draadloze LAN-controller (A) die wordt opgenomen via de functie <u>WLC pakketvastlegging</u>, gecascadeerd met een langere opname van ISE's TCP-dumpen (B). De WLC pakketvastlegging wordt als voorbeeld gebruikt omdat het in omvang meestal zeer klein is.

WLC-pakketvastlegging (A)

📅 radius_novlan.pcap	Pcap Napture	22 KB	Today a	at 11:56 am
ISE-tafelpomp (B)				
adius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm		850 KB	Pcap Napture
Samengesteld (A+B)				
👪 radius_novlan_merged.pcapng	PcapnCapture 9	927 KB	Today at	12:28 pm

Draai vervolgens de straal tegen het samengevoegde pcap (A+B) en u kunt de breedtegraad zien.

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>

Stap 2: PMK(en) uittrekken.

Verwijdert het 0x-veld in elke **MS-MPPE-Recv-Key** van de breedteuitvoer en de PMK's die nodig zijn voor de draadloze verkeersdecode, wordt vervolgens gepresenteerd.

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a 066d8b3b

рмк: ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1b fb0e

Stap 3. Ontdek de OTA-slang.

Navigeer naar Wireless-shark > Voorkeuren > Protocols > IEEE 802.11. Klik vervolgens op Enable Decryption en klik op de knop Bewerken naast Decryptie-toetsen, zoals in de afbeelding weergegeven.

4	Wireshark - Preferences	?	x
HCrt A HDFS HDFSDATA HIP HGnet HGNet HISLIP HL7 HNBAP HPEEDS HSMS HSRP HTTP HTTP2 IAPP IAX2 IB ICAP ICP ICP ICP ICP ICP ICP ICP ICP ICP IC	IEEE 802.11 wireless LAN Reassemble fragmented 802.11 datagrams 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 MIC Length override Edit Decryption keys Edit	Help	

Selecteer vervolgens **wpa-psk** als het Key type en zet de PMK's afgeleid in het **Key** veld, en klik vervolgens op **OK**. Nadat dit is voltooid, dient de OTA-opname te worden decrypteerd en kunt u informatie met een hogere laag (3+) zien.

4	Wireshark - Preferences	? X
	WEP and WPA Decryption Keys ? X	
	Key type Key vypa-psk ddb0b09a7d6980515825950b5929d02/236799f3e8a87f163c8ca41a066d8b3b wpa-psk 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e	
¢	+ - Pa A V R Ckters Administrator HocCata Roaming littreshark (80211 Kevs OK Cancel Help	
	OK Cancel	Help

Voorbeeld van een gedecrypteerd 802.11 Packet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
🗶 🖩 🧷 🐵 📙 🖕 👄 🗠 🐨 🖉 🚛 📄 Q. Q. Q. II	
wian.addr ==04:f1:28:6a:69:11	🔀 🔜 💌 Expression
No. Time Source Destination	Protocol Length Info
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
<u>397884 2018-11-16 00:17:08.098999</u> 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
39/88/ 2018-11-16 00:1/:08.099181 Clsco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (!_ HmdGLODa_ba:69:11 (04:t1:28:ba:69:11) (RA)	802.11 5/ 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
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)	
Radiotap Header v0, Length 48	
882.11 radio information	
> IEEE 802.11 QoS Data, Flags: .pTC	
Logical-Link Control	
Internet Protocol Version 4, Src: 172.16.255.13, Dst: 40.127.66.24	
Transmission Control Protocol, Src Port: 45658, Dst Port: 80, Seq: 128, Ack: 4001196, Len: 0	
010 11 00 00 00 00 00 01 0 00 00 00 00 0	
220 9e 09 0b 22 1f 00 06 00 65 00 00 00 40 00 00 ······e·····	
030 88 41 30 00 00 a3 8e b4 3d e4 04 f1 28 6a 69 11 -A0 = ··(ji-	
040 00 0c 29 28 89 dd 50 06 00 00 c8 84 00 20 01 00 ···)(··P·······	
050 00 00 af f4 c2 2f 90 d1 14 52 a5 8b 2e 57 27 3a	
0660 d8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 34 39 ca T.U49	
5C 08 7a 36 57 cd e2 43 69 86 75 92 24 17 00 00 \ 2004 C ···\$···	
7000 13 67 79 65 61 db a7 06 30 11 16 /0 44 87 5 0 00 11 17 /0 17 17 10 10 10 10 10 10 10 10 10 10 10 10 10	
we de la co la an el an art al	

Als u het tweede resultaat vergelijkt wanneer PMK niet is opgenomen, met het eerste resultaat, wanneer PMK is opgenomen, wordt pakket 397886 gedecrypteerd als 802.11 QoS gegevens.

Voorbeeld van een versleuteld 802.11 Packet

The Source Destination Protocol Length Info 397881 2018-11-16 00:17:08.0980393 Wmare_28:89:dd HidGloba_6a:69:11 802.11 1438 QeS Data, SN=1434, FN=0, Flags=.p 397882 2018-11-16 00:17:08.0980495 HidGloba_6a:69:11 Cisco_b4:3i:4(00:a3:8e:b4:3d:e4) (RA) 802.11 154 QeS Data, SN=1435, FN=0, Flags=.p 397883 2018-11-16 00:17:08.0980495 HidGloba_6a:69:11 Cisco_b4:3i:4(00:a3:8e:b4:3d:e4) (RA) 802.11 154 QeS Data, SN=1435, FN=0, Flags=.p 397884 2018-11-16 00:17:08.099049 HidGloba_6a:69:11 Vmare_28:89:dd 802.11 154 QeS Data, SN=143, FN=0, Flags=.p 397887 2018-11-16 00:17:08.099049 HidGloba_6a:69:11 Vmare_28:89:dd 802.11 154 QeS Data, SN=140, FN=0, Flags=.p 397887 2018-11-16 00:17:08.099059 HidGloba_6a:69:11 Vmare_28:89:dd 802.11 154 QeS Data, SN=02, FN=03, FN=03, FN=03, FN=03, FN=03, FN=03, FN=03, FN=03, FN=04, FN=0, Flags=.p 397887 2018-11-16 00:17:08.099059 HidGloba_6a:69:11 Vmare_28:89:dd 802.11 154 QeS Data, SN=03, SN=03, SN=03, SN=043, SN	Tme: Source Destmoto Protocol Length Info 397881 2018-11-16 00:17:08.098333 Wmare_28:89:dd HidGloba_6a:69:11 802.11 1438 QoS Data, Sh=1434, FN=0, Flags=, p, F. 397882 2018-11-16 00:17:08.098493 HidGloba_6a:69:11 60:10 802.11 5780 QoS Data, Sh=1434, FN=0, Flags=, p, F. 397882 2018-11-16 00:17:08.098494 Wmare_28:89:dd HidGloba_6a:69:11 802.11 5780 QoS Data, Sh=1434, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.099999 HidGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=104, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.099096 HidGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=102, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.09906 HidGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=102, FN=0, Flags=, p, TC 397885 2018-11-16 00:17:08.09905 Cisco_b+13:de:10:17.1 Wmare_28:89:dd 802.11 154 QoS Data, Sh=102, FN=0, Flags=, p, TC 397895 2018-11-16 00:17:08.1082 Cisco_b+13:de:10:16:16:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=, C 397895 2018-11-16 00:17:08.10832 Cisco_b+13:de:10:16:08:6:6:9:11<	.add	==04:f1:28:6a:69:11				X
397881 2012-11-16 00:17:08.098393 Vmmare_28:89:dd HedGloba_6s:69:11 602.11 1438 (05 Data, SH=1434, FN=0, Flags=.p., I 397882 2018-11-16 00:17:08.098495 HmdGloba_6s:69:11 602.11 154 (05 Data, SH=1435, FN=0, Flags=.p., I 397882 2018-11-16 00:17:08.098495 HmdGloba_6s:69:11 Cisco_bat:3die4 (00:a3:8e:b4:3die4) (RA) 802.11 154 (05 Data, SH=145; FN=0, Flags=.p., I 397882 2018-11-16 00:17:08.098495 Wmare_28:89:dd HmdGloba_6s:69:11 802.11 154 (05 Data, SH=14; FN=0, Flags=.p., I 397882 2018-11-16 00:17:08.098495 Wmare_28:89:dd HmdGloba_6s:69:11 802.11 154 (05 Data, SH=14); FN=0, Flags=.p., I 397885 2018-11-16 00:17:08.099181 Cisco_b4:3die4 (00:a3:8e:b4:3die4) (T. HmdGloba_6s:69:11) (AA 802.11 57 802.11 Block Ack, Flags=.p., I 397885 2018-11-16 00:17:08.109055 Cisco_b4:3die4 (00:a3:8e:b4:3die4) (T. HmdGloba_6s:69:11) (AA 802.11 57 802.11 Block Ack, Flags=.p., I 397892 2018-11-16 00:17:08.101762 HmdGloba_6s:69:11 (04:f1:28:6s:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p., I 397892 2018-11-16 00:17:08.101762 HmdGloba_6s:69:11 (04:f1:28:6s:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p., I 397892 2018-11-16 00:17:08.106055 Vmmare_28:89:dd H02 H02 <	397881 2018-11-16 00:17:08.099393 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 1438 QoS Data, SH=1434, FN+0, Flags=.p,F.F. 397881 2018-11-16 00:17:08.099444 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SH=1435, FN+0, Flags=.p,F.F. 397882 2018-11-16 00:17:08.099444 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SH=1435, FN+0, Flags=.p,F.F. 397885 2018-11-16 00:17:08.099445 Wmare_28:89:dd HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 164 QoS Data, SH=1434, FN+0, Flags=.p,F.F. 397885 2018-11-16 00:17:08.099445 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 164 QoS Data, SH=10, FN+0, Flags=.p,TC 397885 2018-11-16 00:17:08.09955 Cisco_P4:3d: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=.p,TC 39789 2018-11-16 00:17:08.010722 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.010724 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.010725 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.010565 Wmare_28:89:dd		Time	Source	Destination	Protocol	Length Info
39782 2018-11-16 00:17:08.098444 Ymaare_28:89:dd HmdGloba_6s:69:11 802.11 154 QoS Data, SN=1435, FN=0, Flags=.p 39788 2018-11-16 00:17:08.098999 Ymaare_28:89:dd HmdGloba_6s:69:11 802.11 154 QoS Data, SN=1435, FN=0, Flags=.p 39788 2018-11-16 00:17:08.098999 Ymaare_28:89:dd HmdGloba_6s:69:11 802.11 154 QoS Data, SN=101, FN=0, Flags=.p 39788 2018-11-16 00:17:08.099909 HmdGloba_6s:69:11 Ymaare_28:89:dd 802.11 154 QoS Data, SN=101, FN=0, Flags=.p 39788 2018-11-16 00:17:08.099605 HmdGloba_6s:69:11 Ymaare_28:89:dd 802.11 154 QoS Data, SN=102, FN=0, Flags=.p 39788 2018-11-16 00:17:08.099505 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6s:69:11) (A4:f1:28:6a:69:11) (RA) 802.11 154 QoS Data, SN=102, FN=0, Flags=.p 39789 2018-11-16 00:17:08.099555 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6s:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C. 39789 2018-11-16 00:17:08.09558 Wmaare_28:89:dd HmdGloba_6s:69:11 S02.11 55 QoS Data, SN=1437, FN=0, Flags=.p 39789 2018-11-16 00:17:08.09558 Wmaare_28:89:dd HmdGloba_6s:69:11 802.11 55 QoS Data, SN=1437, FN=0, Flags=.p 397892 2018-11-16 00:17:08.105558 Wmaare_28:89:dd HmdGloba_6s:69:11<	397822 2018-11-16 00:17:08.09844 Ymmare_28:99:dd HedGloba_6s:69:11 082.11 154 000 Data, SH-Hab, Flags-,,C 397882 2018-11-16 00:17:08.09899 Ymmare_28:09:10 Ymmare_28:09:11 082.11 57 002.11 160 Conta, SH-Hab, Flags-,,C 397886 2018-11-16 00:17:08.098999 Ymmare_28:09:10 Ymmare_28:09:11 082.11 154 000 Data, SH-1435, FH-0, Flags-,,C 397886 2018-11-16 00:17:08.099090 HmdGloba_6s:09:11 082.11 154 000 Data, SH-1435, FH-0, Flags-,,C 397886 2018-11-16 00:17:08.099090 HmdGloba_6s:09:11 082.11 154 000 Data, SH-1435, FH-0, Flags-,,C 397886 2018-11-16 00:17:08.099060 HmdGloba_6s:09:11 082.11 154 000 Data, SH-102, FH-0, Flags-,,C 397895 2018-11-16 00:17:08.09966 HmdGloba_6s:09:11 082.11 154 000 Data, SH-102, FH-0, Flags-,,C 397895 2018-11-16 00:17:08.101762 HmdGloba_6s:09:11 081:11 082.11 154 000 Data, SH-103, FH-0, Flags-,,C 397895 2018-11-16 00:17:08.101762 HmdGloba_6s:09:11 Vmmare_28:09:1d 082.11 154 000 Data, SH-103, FH-0, Flags-,,C 397892 2018-11-16 00:17:08.101762 HmdGloba_6s:09:11 Vmmare_28:09:1d 082.11 590.21 Block Ack, Flags-, SH-135, FH-0, Flags-,,C 397892 2018-11-16 00:17:08.10		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.
397883 2018-11-16 00:17:08.098499 HmdGlobs_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=	397883 2018-11-16 00:17:08.098495 HmdGloba_6s:69:11 (04:f1:28:6a:69:11) Cisco_b4:3d:e4 (00:a):8e:b4:3d:e4 (00:a):8e:b4:3d:e4) 802.11 57 802.11 Block Ack, Flags=C 397884 2018-11-16 00:17:08.099999 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397885 2018-11-16 00:17:08.099999 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397885 2018-11-16 00:17:08.099066 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397885 2018-11-16 00:17:08.099066 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397889 2018-11-16 00:17:08.099066 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397890 2018-11-16 00:17:08.01762 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397891 2018-11-16 00:17:08.01762 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.016056 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.016056 Wmare_28:89:dd HmdGloba_6a:69:11 802.11		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.
397884 2018-11-16 001:71:08.098999 Vmare_28:89:dd HedGloba_6s:69:11 002.11 154 QoS Data, 5N-1405, FN-0, Flags-p 397885 2018-11-16 001:71:08.099909 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 154 QoS Data, 5N-1405, FN-0, Flags-p 397887 2018-11-16 001:71:08.099909 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 154 QoS Data, 5N-1405, FN-0, Flags-p 397887 2018-11-16 001:71:08.099656 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HedGloba_6s:69:11) (04:f1:28:6a:69:11) 002.11 154 QoS Data, 5N=102, FN-0, Flags-p 397889 2018-11-16 001:71:08.100752 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 154 QoS Data, 5N=103, FN=08, Flags-p 397890 2018-11-16 001:71:08.101762 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 157 002.11 Block Ack, Flags 397892 2018-11-16 001:71:08.101762 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 154 QoS Data, SN=103, FN=0, Flagsp 397892 2018-11-16 001:71:08.101762 HedGloba_6s:69:11 Vmare_28:89:dd 002.11 154 QoS Data, SN=1437, FN=0, Flagsp 397892 2018-11-16 001:71:08.10556 Vmare_28:89:dd HedGloba_6s:69:11 002.11 154 QoS Data, SN=1433, FN=0, Flagsp 397894 2018-11-16 001:71:08.106505 Vmare_28:89:dd HedGloba_6s:69:11 002.11 154 QoS Data, SN=1433, FN=0, Flagsp 597894 2018-11-16 001:71:08.106505 Vmare	397884 2018-11-16 00:17:08.099099 Wmare_28:99:dd HudGloba_6s:69:11 002.11 102 006 00:10 114 005 Data, Sh=1436, FH=0, Flags=.ppTC 397886 2018-11-16 00:17:08.099099 HudGloba_6s:69:11 Wmare_28:89:dd 002.11 154 005 Data, Sh=101, FH=0, Flags=.ppTC 397887 2018-11-16 00:17:08.099080 tisco_b4:31:e4 (00:a3:8e:b4:3d:e4) (T.= HudGloba_6s:69:11 (04:f1:28:6s:69:11) (RA) 002.11 57 002.11 DiOck Ack, Flags=.ppTC 397887 2018-11-16 00:17:08.099050 tisco_b4:31:e4 (00:a3:8e:b4:3d:e4) (T.= HudGloba_6s:69:11 (04:f1:28:6s:69:11) (RA) 002.11 57 002.11 DiOck Ack, Flags=.pp,C 397897 2018-11-16 00:17:08.01762 HudGloba_6s:69:11 Wmare_28:89:dd 002.11 479 005 Data, Sh=03, FN=0, Flags=.pp,C 397897 2018-11-16 00:17:08.01762 HudGloba_6s:69:11 (Mmare_28:89:dd 002.11 57 002.11 Block Ack, Flags=.pp,C 397897 2018-11-16 00:17:08.101212 tisco_b4:3:8e:14:3d:e4) (T.= HudGloba_6s:69:11 002.11 57 002.11 Block Ack, Flags=.pp,C 397891 2018-11-16 00:17:08.10555 Wmare_28:89:dd HudGloba_6s:69:11 002.11 57 002.11 Block Ack, Flags=.pp,C 397892 2018-11-16 00:17:08.104555 Wmare_28:89:dd HudGloba_6s:69:11 002.11 59 005 Data, Sh=1435, FN=0, Flags=.pp,F Frame 397886: 154 bytes on wire (1232 bits), 1		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
397886 2018-11-16 00:17:08.099091 HidGlobs_6a:69:11 Vmmare_28:89:dd 802.11 397887 2018-11-16 00:17:08.099081 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 397887 2018-11-16 00:17:08.099081 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 154 QoS Dats, SN=302, FN=6, Flags=.p 397887 2018-11-16 00:17:08.099081 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (RA) 802.11 154 QoS Dats, SN=302, FN=6, Flags=.p 397889 2018-11-16 00:17:08.099055 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (RA) 802.11 154 QoS Dats, SN=303, FN=6, Flags=.p 397891 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p 397891 2018-11-16 00:17:08.101821 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p 397891 2018-11-16 00:17:08.101821 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p 397892 2018-11-16 00:17:08.101821 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11] (RA) 802.11 57 802.11 Block Ack, Flags=.p 397894 2018-11-16 00:17:08.1046055 Vmmare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags=.p 57 802.111-16 00:17:08.1046055 Vmma	397886 2018-11-16 00:17:08.099009 HmdGloba_6s:69:11 Wmare_28:89:dd 082.11 194 QoS Data, SH-101, FH-9, Flags=, pTC 397887 2018-11-16 00:17:08.099050 HmdGloba_6s:69:11 Wmare_28:89:dd 082.11 57 002.11 Block Ack, Flags=, pTC 397887 2018-11-16 00:17:08.099055 Cisco_b4:3ide4 (00:a3:8e:b4:3id:e4) (T. HmdGloba_6s:69:11 (04:f1:28:6a:69:11) (RA) 082.11 57 002.11 Block Ack, Flags=, pTC 397887 2018-11-16 00:17:08.01762 HmdGloba_6s:69:11 Wmare_28:89:dd 082.11 57 002.11 Block Ack, Flags=, pTC 397897 2018-11-16 00:17:08.01052 Cisco_b4:3id:e4 (00:a3:8e:b4:3id:e4) (T. HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 082.11 57 002.11 Block Ack, Flags=, pTC 397897 2018-11-16 00:17:08.01052 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 55 002 Data, SH=437, FH=0, Flags=, p, FL 397897 2018-11-16 00:17:08.01055 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 55 002 Data, SH=437, FH=0, Flags=, p, FL 397897 2018-11-16 00:17:08.10655 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SH=44.78 397886 2018-11-16 00:17:08.10655 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SH=438, FH=0, Flags=, p, FL 397892 2018-11-16 00:17:08.10655 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SH=438, FH=0, Flags=, p, FL 397892 2018-11-16 00:		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.
397887 2018-11-16 00:17:08.099161 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T	397887 2018-11-16 00:17:08.099181 Cisco_b4:34: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= 397888 2018-11-16 00:17:08.099666 HmdGloba_6a:69:11 Wmare_28:89:d4 802.11 57 802.11 Block Ack, Flags=C 397889 2018-11-16 00:17:08.0996656 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 00:17:08.0199655 MmdGloba_6a:69:11 Wmare_28:89:d4 802.11 57 802.11 Block Ack, Flags=C 397891 2018-11-16 00:17:08.019056 Wmare_c28:89:d4 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.019058 Wmare_c28:89:d4 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.019058 Wmare_c28:89:d4 HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags=,C 397894 2018-11:16 00:17:08.106056 Wmare_c28:89:d4 HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags=,C 397894 2018-11:16 00:17:08.106056 Wmare_c28:89:d4 HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags=,F. 202.11 150 00:17:08.106056 Wmare_c28:89:d4 HmdGloba_6a:69:11 802.11 502.11 Block Ack, Flags=,F.		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
397882 2018-11-16 00:17:08.099666 HedGlobs_6a:69:11 Vmware_28:99:dd 802.11 154 QoS Dats, SH=102, FH=0, FHags=.p 397889 2018-11-16 00:17:08.099656 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (P. HmdGlobs_6a:69:11) (P. HmdGlobs_6a:69:11) 802.11 157 802.11 Block Ack, Flags=.p 397891 2018-11-16 00:17:08.10172 HmdGlobs_6a:69:11 Vmware_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p 397891 2018-11-16 00:17:08.10172 Lisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (P. HmdGlobs_6a:69:11) 802.11 57 802.11 Block Ack, Flags=.p 397892 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGlobs_6a:69:11) (P. HmdGlobs_6a:69:11) 802.11 57 802.11 Block Ack, Flags=.p 397892 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGlobs_6a:69:11 802.11 55 005 Data, SH=103, FH=0, Flags=.p 397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGlobs_6a:69:11 802.11 154 QoS Data, SH=104, FH=0, Flags=.p 397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGlobs_6a:69:11 802.11 154 QoS Data, SH=104, FH=0, Flags=.p Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 Dytes captured (1232 bits) 154 Dytes captured (1232 bits) B82.11 radio information Image Capture Capture Capture Capture Capture Capture Capture Ca	397888 2018-11-16 00:17:08.099666 HmdGloba_6s:69:11 Wmware_28:89:dd 802.11 154 (005 Data, 54-102, FM-0, Flags=.pC 397890 2018-11-16 00:17:08.101762 HmdGloba_6s:69:11 Vmware_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397890 2018-11-16 00:17:08.101762 HmdGloba_6s:69:11 Vmware_28:89:dd 802.11 57 802.11 Block Ack, Flags=C 397891 2018-11-16 00:17:08.101812 Cisco_b4:3id:e4 (00:a3:8e:b4:3d:e4) (T		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=
397889 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T	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 00:17:08.01052 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 00:17:08.010550 Vmmare_28:89:d4 HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.10555 Vmmare_28:89:d4 HmdGloba_6a:69:11 802.11 502.11 55 QOS Data, Sh=0437, FH=0, Flags=.pF. 397894 2018-11-16 00:17:08.106556 Vmmare_28:89:d4 HmdGloba_6a:69:11 802.11 802.11 57 802.11 Block Ack, Flags=.pF. 1397894 2018-11-16 00:17:08.106565 Vmmare_28:89:d4 HmdGloba_6a:69:11 802.11 802.11 57 802.11 Block Ack, Flags=.pF. 1adiotap Header v0, Length 48 Vmmare_28:89:d4 HmdGloba_6a:69:11 802.11 802.11 57 802.11 Block Ack, Flags=.pF. 21.11 rddo information Effe 802.11 QoS Data, Flags: .pTC Jata (68 bytes) Jata (100 byte		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 2018-11-16 001:71:08.101762 HmdGlobe_6a:69:11 Vmmare_23:89:dd 802.11 479 QoS Data, SH=103, FH=0, Flags=.p 397891 2018-11-16 001:71:08.10812 Cisco_b4:3d:e4 (00:33:88:b4:3d:e4) (T= HmdGlobe_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p 397892 2018-11-16 001:71:08.106955 Vmmare_28:89:dd HmdGlobe_6a:69:11 802.11 595 QoS Data, SH=1437, FH=0, Flags=.p 397894 2018-11-16 001:71:08.106956 Vmmare_28:89:dd HmdGlobe_6a:69:11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 397895 2018-11-16 001:71:08.106956 Vmmare 28:89:dd HmdGlobe_6a:69:11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 57 802.51 Vmmare 28:89:dd HmdGlobe_6a:69:11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 57 802.51 Vmmare 28:89:dd HmdGlobe_6a:69:11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 57 802.51 Vmmare 28:89:dd HmdGlobe_6a:69:11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 58 802.11 Vmmare 28:89:dd HmdGlobe_6a:69:11 802.11 802.11 154 QoS Data, SN=1438, FH=0, Flags=.p 59 80.51 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 QoS Data, Flags: .p 154 QoS Data, Flags: .p<	397890 2018-11-16 00:17:08.101762 HmdGloba_6::69:11 Wmware_28:89:dd 802.11 479 QoS Data, SH=03, FN=03, FN=03		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 00:17:08.101812 Cisco_b4:30:e4 (40: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=,	397891 2018-11-16 00:17:08.101812 (isco_b4:34:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (8A) 802.11 57 802.11 81ock Ack, Flags=C 397892 2018-11-16 00:17:08.10558 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 QOS Data, SH=1437, FH=0, Flags=.pF. HmdGloba_6a:69:11 802.11 154 Oyt Data, Sh=1438, FH=0, Flags=.pF. Frame 39786: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) addiotap Header v0, Length 48 302.11 radio information EEEE 802.11 QoS Data, Flags: .pTC Data (68 bytes)		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 00:17:08.105958 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1437, FN+0, Flags=.p 397894 2018-11-16 00:17:08.106056 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 1 595 QoS Data, SN=1438, FN+0, Flags=.p rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) its)	397892 2018-11-16 00:17:08.105958 Vmware_28:09:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1437, FN=0, Flags=.pF. 397894 2018-11-16 00:17:08.106056 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 18 802.11 18 802.11 18 402 Data, SN=1438, FN=0, Flags=.pF. irame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) ladiotap Header v0, Length 48 42.11 radio information EEE 802.11 QoS Data, Flags: .pTC lata (68 bytes)		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=.p Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 radio information (EEE 802.11 QoS Data, Flags: .pTC Pata (68 bytes)	397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, 5M=1438, FN=0, Flags=.pF. Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Tadiotap Header V0, Length 48 182.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Tata (68 bytes)		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.
Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) tadiotap Header v0, Length 48 102.11 radio information LEEE 802.11 QoS Data, Flags: .pTC Jata (68 bytes)	Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 102.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Jata (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.
		02.11 EEE 8 ata (µ Header v0, Length 48 radio information 2.11 QoS Data, Flags: .pTC ∴8 bytes)				
00 00 00 30 00 65 00 1c 00 6d f0 30 31 00 00 00 00		Radiot 802.11 IEEE 8 Data (p Header v0, Length 48 madio information 12.11 QoS Data, Flags: .pTC 18 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 30 00 6b 08 1c 00 6d f9 30 31 00	00 00 00 ···0·k··· m·01····			
00 00 00 60 <td< td=""><td></td><td>Radiot 802.11 IEEE 8 Data (00 00 10 14</td><td>p Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 08 30 on 04 22 1f on 06 06 05 30 on 08 30 04</td><td>00 00 00 ······ m··01···· 04 01 00 ·····</td><td></td><td></td><td></td></td<>		Radiot 802.11 IEEE 8 Data (00 00 10 14	p Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 08 30 on 04 22 1f on 06 06 05 30 on 08 30 04	00 00 00 ······ m··01···· 04 01 00 ·····			
00 00 00 05 06 07 00 <td< td=""><td>28 9e 09 0b 22 1f 00 06 05 4 09 4 00 00 00 00 00 00 00 00 00 00 00 00 0</td><td>Radiot 802.11 IEEE 8 Data (00 00 10 14 20 90 30 88</td><td>p Header v0, Length 48 radio information 2.11 QoS Data, Flags: .pTC i8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 44 00 00 00 80 09 9b 02 1f 00 06 00 65 00 00 00 04 13 30 00 80 03 80 b 4 30 40 64 71 23</td><td>00 00 00 ···0·k··· m·01···· 04 01 00 00 00 00 ····· e····· 66 09 11 ···</td><td></td><td></td><td></td></td<>	28 9e 09 0b 22 1f 00 06 05 4 09 4 00 00 00 00 00 00 00 00 00 00 00 00 0	Radiot 802.11 IEEE 8 Data (00 00 10 14 20 90 30 88	p Header v0, Length 48 radio information 2.11 QoS Data, Flags: .pTC i8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 44 00 00 00 80 09 9b 02 1f 00 06 00 65 00 00 00 04 13 30 00 80 03 80 b 4 30 40 64 71 23	00 00 00 ···0·k··· m·01···· 04 01 00 00 00 00 ····· e····· 66 09 11 ···			
00 00 00 60 00 60 00 <td< td=""><td>10 1 + 00 9 5 0 9 00 10 40 9 40 00 00 00 00 00 40 10 00 10 9 6 00 5 0 2 1 f 00 6 00 5 00 6 00 6 00 4 0 0 0 0 0 10 84 1 30 00 80 as be 14 30 as 04 f 1 2 6 a 6 5 11 A0 a (fi 10 00 0 c 2 2 8 9 d d 5 0 6 0 00 0 c 6 8 4 00 2 0 10 0 (f) (P</td><td>Radiot 802.11 IEEE 8 Data (0 00 00 10 14 20 9e 30 88 80 00</td><td>pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 6b 00 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 80 09 b2 21 f0 00 60 00 50 00 00 04 41 30 00 00 a3 0e ba 3d e4 04 f1 28 c 29 28 80 45 06 6 00 0c 88 40 00 c 88 40</td><td>00 00 00 · 0 k · m · 01 · · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></td<>	10 1 + 00 9 5 0 9 00 10 40 9 40 00 00 00 00 00 40 10 00 10 9 6 00 5 0 2 1 f 00 6 00 5 00 6 00 6 00 4 0 0 0 0 0 10 84 1 30 00 80 as be 14 30 as 04 f 1 2 6 a 6 5 11 A0 a (fi 10 00 0 c 2 2 8 9 d d 5 0 6 0 00 0 c 6 8 4 00 2 0 10 0 (f) (P	Radiot 802.11 IEEE 8 Data (0 00 00 10 14 20 9e 30 88 80 00	pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 6b 00 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 80 09 b2 21 f0 00 60 00 50 00 00 04 41 30 00 00 a3 0e ba 3d e4 04 f1 28 c 29 28 80 45 06 6 00 0c 88 40 00 c 88 40	00 00 00 · 0 k · m · 01 · · · · · · · · · · · · · · · · ·			
00 00 <td< td=""><td>110 14 00 96 05 00 <t< td=""><td>Radiot 802.11 IEEE 8 Data (0 10 12 14 20 90 30 88 40 90 50 90</td><td>pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 18 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 00 80 04 d9 44 00 00 00 08 09 0b 22 1f 00 06 00 65 00 00 00 44 1 30 00 00 a3 Be 164 32 d e4 04 f1 23 0c 29 28 89 dd 50 66 00 00 c8 84 00 00 af f4 c2 2f 90 d1 14 52 as 5b 2</td><td>00 00 00 ···0·k··· m·01···· 04 01 00 00 00 00 ···· c 66 69 11 ···0 ··· c 66 69 11 ···0 ··· (ji 20 01 00 ···)(··P ·····)':</td><td></td><td></td><td></td></t<></td></td<>	110 14 00 96 05 00 <t< td=""><td>Radiot 802.11 IEEE 8 Data (0 10 12 14 20 90 30 88 40 90 50 90</td><td>pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 18 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 00 80 04 d9 44 00 00 00 08 09 0b 22 1f 00 06 00 65 00 00 00 44 1 30 00 00 a3 Be 164 32 d e4 04 f1 23 0c 29 28 89 dd 50 66 00 00 c8 84 00 00 af f4 c2 2f 90 d1 14 52 as 5b 2</td><td>00 00 00 ···0·k··· m·01···· 04 01 00 00 00 00 ···· c 66 69 11 ···0 ··· c 66 69 11 ···0 ··· (ji 20 01 00 ···)(··P ·····)':</td><td></td><td></td><td></td></t<>	Radiot 802.11 IEEE 8 Data (0 10 12 14 20 90 30 88 40 90 50 90	pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 18 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 00 80 04 d9 44 00 00 00 08 09 0b 22 1f 00 06 00 65 00 00 00 44 1 30 00 00 a3 Be 164 32 d e4 04 f1 23 0c 29 28 89 dd 50 66 00 00 c8 84 00 00 af f4 c2 2f 90 d1 14 52 as 5b 2	00 00 00 ···0·k··· m·01···· 04 01 00 00 00 00 ···· c 66 69 11 ···0 ··· c 66 69 11 ···0 ··· (ji 20 01 00 ···)(··P ·····)':			
00 00 <td< td=""><td>110 14 00 96 00 <t< td=""><td>Radiot 802.11 IEEE 8 Data (000 000 10 14 200 90 30 88 440 000 50 000 60 d8</td><td>pp Header v0, Length 48 radio information 22.11 QoS Data, Flags: .pTC i8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 10 80 04 d9 44 60 00 00 00 80 09 9e 21 1f 00 06 00 65 80 00 00 41 13 00 00 80 38 66 00 00 c8 84 00 00 60 47 4 c2 27 90 41 14 52 a5 80 22 4 a5 55 00 a1 29 24 af c6 a9 1f c2 c8 4 a5 55 00 12 92 4a fc a of a fc c2 c8</td><td>00 00 00 -0 k - m 01 00 01 000 - c</td><td></td><td></td><td></td></t<></td></td<>	110 14 00 96 00 <t< td=""><td>Radiot 802.11 IEEE 8 Data (000 000 10 14 200 90 30 88 440 000 50 000 60 d8</td><td>pp Header v0, Length 48 radio information 22.11 QoS Data, Flags: .pTC i8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 10 80 04 d9 44 60 00 00 00 80 09 9e 21 1f 00 06 00 65 80 00 00 41 13 00 00 80 38 66 00 00 c8 84 00 00 60 47 4 c2 27 90 41 14 52 a5 80 22 4 a5 55 00 a1 29 24 af c6 a9 1f c2 c8 4 a5 55 00 12 92 4a fc a of a fc c2 c8</td><td>00 00 00 -0 k - m 01 00 01 000 - c</td><td></td><td></td><td></td></t<>	Radiot 802.11 IEEE 8 Data (000 000 10 14 200 90 30 88 440 000 50 000 60 d8	pp Header v0, Length 48 radio information 22.11 QoS Data, Flags: .pTC i8 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 09 80 04 d9 44 60 00 00 00 80 09 9e 10 80 04 d9 44 60 00 00 00 80 09 9e 21 1f 00 06 00 65 80 00 00 41 13 00 00 80 38 66 00 00 c8 84 00 00 60 47 4 c2 27 90 41 14 52 a5 80 22 4 a5 55 00 a1 29 24 af c6 a9 1f c2 c8 4 a5 55 00 12 92 4a fc a of a fc c2 c8	00 00 00 -0 k - m 01 00 01 000 - c			
00 00 00 60 00 <td< td=""><td>111 14 00 96 <t< td=""><td>Radiot 802.11 IEEE 8 Data (00 00 10 14 20 9e 30 88 40 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00</td><td>pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 a4 00 00 00 00 80 09 b2 21 f0 00 60 00 50 00 80 09 b2 21 60 06 00 60 00 68 04 41 30 00 00 a3 8c ba 3d a4 04 64 f1 28 0c 29 28 80 45 66 6 00 cc 88 40 00 af f4 c2 2f 90 d1 14 52 a5 16 26 84 a5 55 00 a1 29 24 af cs 09 1f c2 63 85 7 cd c2 43 89 86 f5 92 24 7 cd c 27 cd c2 43 89 86 f5 92 24</td><td>00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></t<></td></td<>	111 14 00 96 <t< td=""><td>Radiot 802.11 IEEE 8 Data (00 00 10 14 20 9e 30 88 40 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00</td><td>pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 a4 00 00 00 00 80 09 b2 21 f0 00 60 00 50 00 80 09 b2 21 60 06 00 60 00 68 04 41 30 00 00 a3 8c ba 3d a4 04 64 f1 28 0c 29 28 80 45 66 6 00 cc 88 40 00 af f4 c2 2f 90 d1 14 52 a5 16 26 84 a5 55 00 a1 29 24 af cs 09 1f c2 63 85 7 cd c2 43 89 86 f5 92 24 7 cd c 27 cd c2 43 89 86 f5 92 24</td><td>00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></t<>	Radiot 802.11 IEEE 8 Data (00 00 10 14 20 9e 30 88 40 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00 50 00	pp Header v0, Length 48 radio information 12.11 QoS Data, Flags: .pTC 8 bytes) 00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 a4 00 00 00 00 80 09 b2 21 f0 00 60 00 50 00 80 09 b2 21 60 06 00 60 00 68 04 41 30 00 00 a3 8c ba 3d a4 04 64 f1 28 0c 29 28 80 45 66 6 00 cc 88 40 00 af f4 c2 2f 90 d1 14 52 a5 16 26 84 a5 55 00 a1 29 24 af cs 09 1f c2 63 85 7 cd c2 43 89 86 f5 92 24 7 cd c 27 cd c2 43 89 86 f5 92 24	00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·			

Voorzichtig: U kunt bij decryptie problemen krijgen met Wireshark en in dat geval, zelfs als de juiste PMK is geleverd (of als PSK wordt gebruikt, zowel SSID als PSK worden geleverd), decrypteert Wireshark de OTA opname niet. Het programma is om Wireless-shark uit en op een paar keer uit te schakelen totdat meer laaginformatie kan worden verkregen en de pakketten 802.11 niet langer als QoS-gegevens worden weergegeven, of om een andere PC/Mac te gebruiken waar Wireless-shark is geïnstalleerd.

Tip: een C++ code genaamd pmkXtract is aangesloten in de eerste post op Gerelateerde informatie. Pogingen om samen te stellen werden succesvol en een uitvoerbaar bestand wordt verkregen, maar het uitvoerbare programma lijkt de decryptie niet goed uit te voeren om een paar onbekende redenen. Daarnaast is er een Python-script dat probeert PMK te extraheren in het commentaar op de eerste post, dat nader kan worden onderzocht indien de lezers geïnteresseerd zijn.

Gerelateerde informatie

- De zwakke link van EAP bijsnijden het zuigen van WiFi-PMK's met pmkXtract
- Hoe Decode Radius MS-MPPE-Recv-Key moet worden gedecodeerd
- Technische ondersteuning en documentatie Cisco Systems