

Wi-Fi

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

http

No.	Time	Source	Destination	Protocol	Length	Info
284	69.261929	192.168.43.221	104.71.116.51	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
290	69.339180	104.71.116.51	192.168.43.221	HTTP/XL	547	HTTP/1.1 200 OK
3204	183.842617	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAiIzVJfGSRETRS1gpHeuVI%3D HTTP/...
3207	183.920868	117.18.237.29	192.168.43.221	OCSP	519	Response
3454	213.214509	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAi4e1AbvpzaLRZNPj1Rv1U%3D HTTP/...
3457	213.307948	117.18.237.29	192.168.43.221	OCSP	519	Response

> Frame 284: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF\_{026754C8-DE61-4CEF-A4EC-E01FB317B8B4}, id 0

> Ethernet II, Src: LiteonTe\_bf:2b:63 (50:5b:c2:bf:2b:63), Dst: XiaomiCo\_45:36:d0 (d8:32:e3:45:36:d0)

> Internet Protocol Version 4, Src: 192.168.43.221, Dst: 104.71.116.51

> Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

Source Port: 54510

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 213]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3311358281

[Next sequence number: 214 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 754605265

0101 .... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 513

0000 d8 32 e3 45 36 d0 50 5b c2 bf 2b 63 08 00 45 00 -2-E6 P...+c-E-

0010 00 fd 16 ef 40 00 80 06 1a 0c c0 a8 2b dd 68 47 ....@...+hG

0020 74 33 d4 ee 00 50 c5 5f 51 49 2c fa 5c d1 50 18 t:LP\_Q,;P-

0030 02 01 65 f4 00 00 47 45 54 20 2f 65 6e 2d 55 53 ..e...GET/en-US

0040 2f 6c 69 76 65 74 69 6c 65 2f 70 72 65 69 6e 73 /livetile/preins

0050 74 61 6c 6c 3f 72 65 67 69 6f 6e 3d 55 53 26 61 tall?reg ion=US&a

0060 70 70 69 64 3d 43 39 38 45 41 35 42 30 38 34 32 ppid=C98 EA5B0842

0070 44 42 42 39 34 30 35 42 42 46 30 37 31 45 31 44 DBB9405B BF071E1D

0080 41 37 36 35 31 32 44 32 31 46 45 33 36 26 46 4f A76512D2 1FE36&FO

0090 52 4d 3d 54 68 72 65 73 68 6f 6c 64 20 48 54 54 RM=Thres hold HTT

00a0 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f P/1.1..C onnectio

00b0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 n: Keep- Alive..U

00c0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f ser-Agen t: Micro

00d0 73 6f 66 74 2d 57 4e 53 2f 31 30 2e 30 0d 0a 48 soft-WNS /10.0..H

00e0 6f 73 74 3a 20 74 69 6c 65 2d 73 65 72 76 69 63 ost: tile-servic

00f0 65 2e 77 65 61 74 68 65 72 2e 6d 69 63 72 6f 73 e.weather.micros

0100 6f 66 74 2e 63 6f 6d 0d 0a 0d 0a oft.com-...

Hypertext Transfer Protocol: Protocol

Packets: 6272 · Displayed: 6 (0.1%)

Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
284	69.261929	192.168.43.221	104.71.116.51	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
290	69.339180	104.71.116.51	192.168.43.221	HTTP/X	547	HTTP/1.1 200 OK
3204	183.842617	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAiIzVJfGSRETRS1gpHeuVI%3D HTTP/...
3207	183.920868	117.18.237.29	192.168.43.221	OCSP	519	Response
3454	213.214509	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAi4e1AbvpzaLRZNPj1Rv1U%3D HTTP/...
3457	213.307948	117.18.237.29	192.168.43.221	OCSP	519	Response

> Ethernet II, Src: LiteonTe\_bf:2b:63 (50:5b:c2:bf:2b:63), Dst: XiaomiCo\_45:36:d0 (d8:32:e3:45:36:d0)

> Internet Protocol Version 4, Src: 192.168.43.221, Dst: 104.71.116.51

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 253
- Identification: 0x16ef (5871)
- > Flags: 0x4000, Don't fragment
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x1a0c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.43.221
- Destination: 104.71.116.51

> Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

```
0000 d8 32 e3 45 36 d0 50 5b c2 bf 2b 63 08 00 45 00  .2.E6.Pf...+c..E-
0010 00 fd 16 ef 40 00 80 06 1a 0c 00 a8 2b dd 68 47  .-...0...+..hG
0020 74 33 d4 ee 00 50 c5 5f 51 49 2c fa 5c d1 50 18  t3...P_ QI,.-\P-
0030 02 01 65 f4 00 00 47 45 54 20 2f 65 6e 2d 55 53  ..e...GE T /en-US
0040 2f 6c 69 76 65 74 69 6c 65 2f 70 72 65 69 6e 73  /livetile/preins
0050 74 61 6c 6c 3f 72 65 67 69 6f 6e 3d 55 53 26 61  tall?reg ion=US&a
0060 70 70 69 64 3d 43 39 38 45 41 35 42 30 38 34 32  ppid=C98 EA5B0842
0070 44 42 42 39 34 30 35 42 42 46 30 37 31 45 31 44  DBB9405B BF071E1D
0080 41 37 36 35 31 32 44 32 31 46 45 33 36 26 46 4f  A76512D2 1FE36&FO
0090 52 4d 3d 54 68 72 65 73 68 6f 6c 64 20 48 54 54  RM=Thres hold HTT
00a0 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f  P/1.1..C onnectio
00b0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55  n: Keep- Alive- U
00c0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f  ser-Agen t: Micro
00d0 73 6f 66 74 2d 57 4e 53 2f 31 30 2e 30 0d 0a 48  soft-WNS /10.0..H
00e0 6f 73 74 3a 20 74 69 6c 65 2d 73 65 72 76 69 63  ost: tile-servic
00f0 65 2e 77 65 61 74 68 65 72 2e 6d 69 63 72 6f 73  e.weather.micros
0100 6f 66 74 2e 63 6f 6d 0d 0a 0d 0a  oft.com- ...
```

Hypertext Transfer Protocol: Protocol

Packets: 8251 · Displayed: 14 (0.2%)

Profile: Default



Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
284	69.261929	192.168.43.221	104.71.116.51	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
290	69.339180	104.71.116.51	192.168.43.221	HTTP/X	547	HTTP/1.1 200 OK
3204	183.842617	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAiIzVJfGSRETRS1gpHeuVI%3D HTTP/...
3207	183.920868	117.18.237.29	192.168.43.221	OCSP	519	Response
3454	213.214509	192.168.43.221	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHwMys%2BghUNoZ7OrUETfACEAi4e1AbvpzaLRZNPj1Rv1U%3D HTTP/...
3457	213.307948	117.18.237.29	192.168.43.221	OCSP	519	Response

> Frame 284: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF\_{026754C8-DE61-4CEF-A4EC-E01FB317B8B4}, id 0

> Ethernet II, Src: LiteonTe\_bf:2b:63 (50:5b:c2:bf:2b:63), Dst: XiaomiCo\_45:36:d0 (d8:32:e3:45:36:d0)

> Internet Protocol Version 4, Src: 192.168.43.221, Dst: 104.71.116.51

> Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 213

Hypertext Transfer Protocol

> GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft-WNS/10.0\r\nHost: tile-service.weather.microsoft.com\r\n\r\n[Full request URI: http://tile-service.weather.microsoft.com/en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold]  
[HTTP request 1/1]  
[Response in frame: 290]

0000	d8 32 e3 45 36 d0 50 5b c2 bf 2b 63 08 00 45 00	-2-E6-P[...+c...E-
0010	00 fd 16 ef 40 00 80 06 1a 0c c0 a8 2b dd 68 47	....@...+..hG
0020	74 33 d4 ee 00 50 c5 5f 51 49 2c fa 5c d1 50 18	t3...P..._QI,...\P-
0030	02 01 65 f4 00 00 47 45 54 20 2f 65 6e 2d 55 53	--e...GE T /en-US
0040	2f 6c 69 76 65 74 69 6c 65 2f 70 72 65 69 6e 73	/livetile/preins
0050	74 61 6c 6c 3f 72 65 67 69 6f 6e 3d 55 53 26 61	tall?reg ion=US&a
0060	70 70 69 64 3d 43 39 38 45 41 35 42 30 38 34 32	ppid=C98 EA5B0842
0070	44 42 42 39 34 30 35 42 42 46 30 37 31 45 31 44	DBB9405B BF071E1D
0080	41 37 36 35 31 32 44 32 31 46 45 33 36 26 46 4f	A76512D2 1FE36&FO
0090	52 4d 3d 54 68 72 65 73 68 6f 6c 64 20 48 54 54	RM=Thres hold HTT
00a0	50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f	P/1.1..C onnectio
00b0	6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55	n: Keep- Alive..U
00c0	73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f	ser-Agen t: Micro
00d0	73 6f 66 74 2d 57 4e 53 2f 31 30 2e 30 0d 0a 48	soft-WNS /10.0..H
00e0	6f 73 74 3a 20 74 69 6c 65 2d 73 65 72 76 69 63	ost: til e-servic
00f0	65 2e 77 65 61 74 68 65 72 2e 6d 69 63 72 6f 73	e.weathe r.micros
0100	6f 66 74 2e 63 6f 6d 0d 0a 0d 0a	oft.com+ ...

Hypertext Transfer Protocol (http), 213 bytes

Packets: 10907 · Displayed: 42 (0.4%)

Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
362	34.571211	2405:204:9726:4e96::...	2404:6800:4009:80c::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=15, hop limit=128 (reply in 363)
363	34.664263	2404:6800:4009:80c::...	2405:204:9726:4e96::...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=15, hop limit=117 (request in 362)
364	35.586888	2405:204:9726:4e96::...	2404:6800:4009:80c::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=16, hop limit=128 (reply in 365)
365	35.649122	2404:6800:4009:80c::...	2405:204:9726:4e96::...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=16, hop limit=117 (request in 364)
366	38.145227	XiaomiCo_45:36:d0	LiteonTe_bf:2b:63	ARP	42	Who has 192.168.43.221? Tell 192.168.43.1
367	38.145257	LiteonTe_bf:2b:63	XiaomiCo_45:36:d0	ARP	42	192.168.43.221 is at 50:5b:c2:bf:2b:63
368	38.624563	fe80::da32:e3ff:fe4...	2405:204:9726:4e96::...	ICMPv6	86	Neighbor Solicitation for 2405:204:9726:4e96:6c92:56f3:4758:a907 from d8:32:e3:45:36:d0
369	38.624953	2405:204:9726:4e96::...	fe80::da32:e3ff:fe4...	ICMPv6	86	Neighbor Advertisement 2405:204:9726:4e96:6c92:56f3:4758:a907 (sol, ovr) is at 50:5b:c2:bf:2b:63
370	38.999687	2405:204:9726:4e96::...	2a01:111:f100:7000::...	TLSv1.2	131	Application Data
371	39.124710	2a01:111:f100:7000::...	2405:204:9726:4e96::...	TLSv1.2	120	Application Data
372	39.164900	2405:204:9726:4e96::...	2a01:111:f100:7000::...	TCP	74	54358 → 443 [ACK] Seq=58 Ack=47 Win=512 Len=0

> Frame 362: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF\_{026754C8-DE61-4CEF-A4EC-E01FB317BBB4}, id 0

> Ethernet II, Src: LiteonTe\_bf:2b:63 (50:5b:c2:bf:2b:63), Dst: XiaomiCo\_45:36:d0 (d8:32:e3:45:36:d0)

> Internet Protocol Version 6, Src: 2405:204:9726:4e96:6c92:56f3:4758:a907, Dst: 2404:6800:4009:80c::200e

Internet Control Message Protocol v6

Type: Echo (ping) request (128)

Code: 0

Checksum: 0x2116 [correct]

[Checksum Status: Good]

Identifier: 0x0001

Sequence: 15

[Response In: 363]

Data (32 bytes)

```
0000 d8 32 e3 45 36 d0 50 5b c2 bf 2b 63 86 dd 60 00  -2.E6.P[ ...+c...
0010 00 00 00 28 3a 80 24 05 02 04 97 26 4e 96 6c 92  ...(:.$- ...&N.l-
0020 56 f3 47 58 a9 07 24 04 68 00 40 09 08 0c 00 00  V-GX-.$- h.@-...
0030 00 00 00 00 20 0e 80 00 21 16 00 01 00 0f 51 62  ....[!][ ][b
0040 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72  cdefghij klmnopqr
0050 73 74 75 76 77 61 62 63 64 65 66 67 68 69      stuvwabc defghi
```

wireshark\_Wi-Fi\_20200830222252\_a12656.pcapng

Packets: 380 · Displayed: 380 (100.0%) · Dropped: 0 (0.0%)

Profile: Default



Page 10 of 10

▼ User Datagram Protocol, Src Port: 53437, Dst Port: 443

```
> Data (33 bytes)
```

0000	d8 32 e3 45 36 d0 50 5b	c2 bf 2b 63	86 dd	60 07	2 E6 P	+	
0010	73 8b 00 29 11 a0 24 05	02 04 97 26	4e 96	6c 92	s - ) @s	&N 1	
0020	56 f3 47 58 a9 07 24 04	68 00 04 09	08 09	00 00	V GX - \$	h -	
0030	00 00 00 00 20 0e d0 bd	01 bb 00 29	10 46	48 ff			
0040	1d 61 bf f7 c9 31 ea 61	5e b5 03 ba	ba 3c	5d 26	a - a 1 a	&	
0050	16 f4 9d 00 26 a0 10 b6	6c d8 18 fa	bf 36	49	6 - - -	1 -	6T

Profile: Default