# LWAPP는 WildPackets OmniPeek 및 EtherPeek 3.0 소프트웨어에서 지원 기능을 디코딩합니다.

#### 목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>LWAPP 디코드 파일 수정</u> <u>TCP UDP Ports.dcd 수정</u> <u>Pspecs.xml 파일 수정</u> <u>OmniPeek 5.0의 LWAPP 디코딩</u> <u>다음을 확인합니다.</u> <u>관련 정보</u>

### <u>소개</u>

WildPackets OmniPeek(및 EtherPeek)은 LWAPP(Lightweight Access Point Protocol) 디코딩을 사용할 수 있지만 연결되지 않습니다. 이 문서에서는 LWAPP 디코딩을 활성화하고 소프트웨어를 사용하여 LWAPP를 보는 방법에 대해 설명합니다. 이 문서에서는 EtherPeek 3.0 및 OmniPeek 5.0에 대한 절차를 사용합니다.

참고: OmniPeek 3.0의 절차는 EtherPeek 3.0의 절차와 동일합니다.

참고: OmniPeek와 EtherPeek 소프트웨어의 유일한 차이점은 파일의 위치입니다.

- OmniPeek의 경로는 C:/Program Files/WildPackets/OmniPeek입니다.
- EtherPeek의 경로는 C:/Program Files/WildPackets/EtherPeek입니다.

# <u>사전 요구 사항</u>

#### <u>요구 사항</u>

EtherPeek, OmniPeek 3.0 및 5.0 소프트웨어에 대해 알고 있는 것이 좋습니다. EtherPeek에 대한 자세한 내용은 EtherPeek <u>FAQ를</u> 참조하십시오 . OmniPeek에 대한 자세한 내용은 <u>Introducing</u> <u>Omni 를</u> 참조하십시오.

#### <u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

#### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙을 참고하십시오.</u>

### <u>LWAPP 디코드 파일 수정</u>

LWAPP 디코딩 파일을 수정하려면 LWAPP 함수에 "ETR 0 0 90 c2 AP Identity:;"을 추가합니다. 이 것은 LWAPP-light\_weight\_의 "LAPL 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" 줄 바로 아래에 있습니다.protocol.dcd 파일(C:\Program Files\WildPackets\EtherPeek\Decodes).

### <u>TCP\_UDP\_Ports.dcd 수정</u>

TCP\_UDP\_Ports.dcd(C:\Program Files\WildPackets\EtherPeek\Decodes) 파일에서 다음 두 행을 포함해야 합니다.

0x2fbe | LWAPP;

0x2fbf | LWAPP;

**참고:** 이 프로세스의 결과로 호스트 컴퓨터에 포트가 열려 있지 않습니다. 따라서 이 단계에서는 호 스트 컴퓨터가 보안 위험에 노출되지 않습니다.

이러한 방식으로 12222와 12223 2개의 포트가 포함됩니다.

#### Pspecs.xml 파일 수정

다음 단계를 완료하십시오.

1. pspecs.xml(C:\Program Files\WildPackets\EtherPeek\1033) 파일의 UDP(User Datagram Protocol) 섹션에서 다음 행을 추가합니다.**참고:** 먼저 원본 파일을 백업해야 합니다.

```
<PSpec Name="LWAPP">
  <PSpecID>6677</PSpecID>
  <LName>LWAPP</LName>
  <SName>LWAPP</SName>
  <Desc>LWAPP</Desc>
  <Color>color_1</Color>
  <CondSwitch>12222</CondSwitch>
  <CondSwitch>12223</CondSwitch>
     <PSpec Name="LWAPP Data">
<PSpecID>6688</PSpecID>
<LName>LWAPP Data</LName>
<SName>LWAPP-D</SName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12222) || (DestPort == 12222)]]></CondExp>
     </PSpec>
     <PSpec Name="LWAPP Control">
```

<PSpecID>6699</PSpecID>

```
<LName>LWAPP Control</LName>
```

```
<SName>LWAPP-C</SName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
</PSpec>
</PSpec>
```

2. 변경 사항을 적용하려면 OmniPeek 또는 EtherPeek를 다시 시작하십시오.

### <u>OmniPeek 5.0의 LWAPP 디코딩</u>

OmniPeek 버전 5.0은 OmniPeek 버전 3.0의 차세대 캡처 툴입니다. 5.0 버전에서는 기본적으로 LWAPP 디코딩이 내장되어 있습니다. 따라서 파일에서 더 이상 변경할 필요가 없습니다. 그러나 IP 주소 및 포트 번호를 사용하여 5.0 버전에서 프로토콜 필터를 정의하는 방법을 보여 주는 예는 다음 과 같습니다.

- 1. OmniPeek 5.0 응용 프로그램을 엽니다.
- 2. Start(시작) 페이지에서 File(파일) > New(새로 만들기)를 클릭하여 New Packet Capture Window(새 패킷 캡처 창)를 엽니다.Capture Options라는 작은 창이 나타납니다. 여기에는 패 킷 캡처에 대한 옵션 목록이 포함됩니다.
- 3. Adapter 옵션에서 해당 어댑터를 사용하여 Capture Packets를 캡처할 어댑터를 선택합니다. 어댑터에 대한 설명은 어댑터를 강조 표시할 때 아래에 표시됩니다. 로컬 이더넷 어댑터를 사용하여 패킷을 캡처하려면 Local Area Connection을 선택합니다.
- 4. 확인을 클릭합니다.New Capture(새 캡처) 창이 나타납니다.
- 5. Start Capture(캡처 **시작)** 버튼을 클릭합니다.툴은 소프트웨어에 정의된 프로토콜에 대한 패킷 을 캡처하기 시작합니다. 캡처된 패킷을 보려면 왼쪽의 Capture 메뉴 아래에 있는 Packets 옵 션을 클릭합니다.
- 6. 캡처된 패킷 중 하나를 마우스 오른쪽 버튼으로 클릭하고 **Make Filter를** 클릭하여 새 프로토콜 을 정의합니다.Insert Filter 창이 나타납니다.
- 7. 프로토콜을 식별하려면 Filter 상자 안에 이름을 입력합니다.주소 필터를 활성화합니다.Type as IP를 선택하여 특정 IP 주소 간에 패킷을 캡처합니다.Address1에 소스 IP 주소를 입력합니 다.주소 2의 경우 대상에 고정 IP가 있는 경우 IP 주소를 입력합니다.목적지가 DHCP를 통해 IP 주소를 수신하는 경우 Option as Any Address를 선택합니다.패킷 흐름의 방향을 지정하려 면 Both directions 버튼을 클릭하고 세 가지 옵션 중 하나를 선택합니다. 단추의 화살표 표시는 선택한 방향을 나타냅니다.포트 필터를 활성화합니다.프로토콜에서 사용하는 포트의 Type(유 형)을 선택합니다(예: TCP).포트 1에 소스에 사용된 포트를 입력합니다.목적지에서 잘 정의된 표준 포트를 사용하는 경우 Port 2에 포트 번호를 입력합니다.그렇지 않으면 목적지가 임의의 기준으로 포트를 사용하는 경우 Any port 옵션을 선택합니다.요구 사항에 따라 Both Directions 버튼에서 방향을 선택합니다.
- 8. 새 사용자 지정 프로토콜을 정의하려면 이 단계를 반복합니다.

# <u>다음을 확인합니다.</u>

OmniPeek 5.0을 사용하면 LWAPP 이벤트가 트리거될 때 Capture Screen에서 툴이 기본적으로 LWAPP 프로토콜을 캡처하는지 확인할 수 있습니다. <u>그림 1</u>은 LAP에서 수행한 검색 요청 중 LWAPP 프로토콜 캡처를 보여줍니다.

ay res con terr	Capture send monitor room	s weithin upp .					
🗟 - 😫 - 📮	🛛 🗙 🖪 🗶 📣 🦚	8720001	- P . 3	0	👌 🥥 Buy Now		
Packets received	707 Buffer un	age: 19%		a franciska se		half the second shall be defined by a	Benefat a la la
Packets filtered:	207 Filter si	tates 🗰 Accept all packets					Sale Capitan
7-							
= Capture	da an 110 51 62 103		10.0	12	reesen and a second		
Deshboard				1.00	and the second second	and a second	
Packets	Source	Desthation	Plags	204	Relative Tane	PTOROCOL	Stemark
Log	3 10.77.244.209	IF Broadcast		96	0:01:10.277675	DW3	C OUEPT NAME-CISCO-LWAPF-CONTROL
fikers	#POD:1A:A1:54:30:AB	Moast 802.1d Br	•	64	0:01:11.067006	002.1	
≥ Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	syslog	SEC=60909,D#t= 514 ,L= 122
Herarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	syslog	SIC+60909,D#5* 514 ,L* 95
Flat	3 10.77.244.209	IF Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t= 514 ,L= 91
Application	#900:1A:A1:54:30:AB	Monst 802.1d Br	•	64	0:01:13.072054	002.1	
😹 Web	3 10.77.244.209	IP Broadcast		96	0:01:13.277035	08/5	C QUERT NAME+CISCO-LWAPP-CONTROL
Servers	B900:1A:A1:54:30:AB	Boast 802.1d Br	•	64	0:01:15.077120	-802.1	
Clerks	3 10.77.244.209	IF Buoadcast		96	0:01:16.275883	DWS	C OUEPT NAME-CISCO-LWAPP-CONTROL
Pages	#00:1A:A1:54:30:AB	Mast 802.14 Br	•	64	0:01:17.081615	002.1	
Requests	B900:1A:A1:54:30:AB	Mp Mcast 802.1d Sr	•	64	0:01:19.088698	-802.1	
🗟 Voice & Video	B900:18:D4:E3:A8:18	Ethernet Scoadcast		64	0:01:19,275905	ARP Request	10.77.244.204 + 7
Calls	2900:1A:A1:54:30:AB	20011A1A11541301A8		64	0:01:20.042094	Loopback	
Media	10.77.244.209	IP Broadcast		151	0:01:20.274975	syslog	SEC-60909,Det+ 514 ,L+ 105
R Visuals	10.77.244.209	IF Broadcast		156	0:01:20.275459	syslog	Scc+60909,Dat+ 514 ,L+ 110
Apdex	3 10.77.244.209	🚼 I? Bzosdcast		146	0:01:20.276394	LVAPP	15co+14977,0st+12223 ,L+ 100
Peer Map	2900:1A1A1:54:30:A8	MAASC 802.14 St		64	0:01:21.090924	002.1	
Graphs	BO0:1A:A1:54:30:AB	BRCast 002.1d Bg		64	0:01:23.095938	002.1	
Statistics	B00:1A:A1:54:30:AB	20110010C1CC1CC1CC		64	0:01:23.481099	00-00-00-20-04	
Nodes	\$900:1A:A1:54:30:A8	E01:00:0C100:00:00		-94	0:01:23.481160	00-00-00-00-03	
Protocols	B900:1A:A1:54:30:A5	BROAST 802.14 BE	. *	64	0:01:25.102850	002-1	
Summary	#900:1A:A1:54:30:AB	Boast 802.1d BE		64	0101:27.107696	802-1	
	##00:1A:A1:54:30:AB	My Mcast 802.1d Sr		64	0:01:29.112083	802-1	
	200:1A:A1:54:30:AB	200:1A:A1:54:30:A3		64	0:01:30.051235	Loopback	
	B00:18:D4:E3:A8:18	Ethernet Broadcast		- 64	0:01:30.292150	APP Request	10.77.244.203 - 7
	#900:1A:A1:54:30:AB	Minest 002.1d Bc		64	0:01:31.116975	802.1	
	#900:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:31.291080	ARP Request	10.77.244.203 - 2
	200:1A:A1:54:30:A8	Mast 802.14 St		64	0:01:33.122176	802.1	
	10.77.244.209	2 1P Buoadcast		132	0:01:34.336071	sysiog	frc-60909,Dst= 514 ,L= 66
	9 10.77.244.209	TF Broadcast		132	0:01:34.336407	#7#10g	Szc=60909,Det= 514 ,L= 00
	#900:1A:A1:54:30:AB	My Mcest 802.14 Br	*	64	0:01:35.126796	802.1	
	10.77.244.209	IF Scondcast		132	0:01:35.348150	syslog	Src=60909,Dst= 514 ,L= 66
	100:1A:A1:54:30:AB	Brast 802.1d Br		64	0:01:37.135293	802.1	
					P		the second second second

패킷에 대한 세부 정보를 보려면 패킷을 두 번 클릭합니다.

# <u>관련 정보</u>

- EtherPeek FAQ
- <u>옴니 소개</u>
- <u>OmniPeek 5.0 다운로드</u>
- <u>기술 지원 및 문서 Cisco Systems</u>