

CAPTURING DIS PACKETS

For analysis it is often useful to capture DIS packets as they are sent over ethernet. This can be achieved using software that captures all network traffic on a specific network device. Useful software for this purpose is Wireshark (WireShark, n.d.).

One possible use case for capturing DIS packets might be the following: DIS packets are broadcast from a local machine running a Coalition Battle Management Language (CBML) application (IP: 192.168.188.87) to the broadcast address of the local network (IP: 192.168.188.255).

After installing Wireshark to a machine on the local network, Wireshark must be started. The startup screen of Wireshark shows a selection dialog (Figure 36) for the target network interface to capture packets from. For most of our LVC environments it is the ethernet interface.

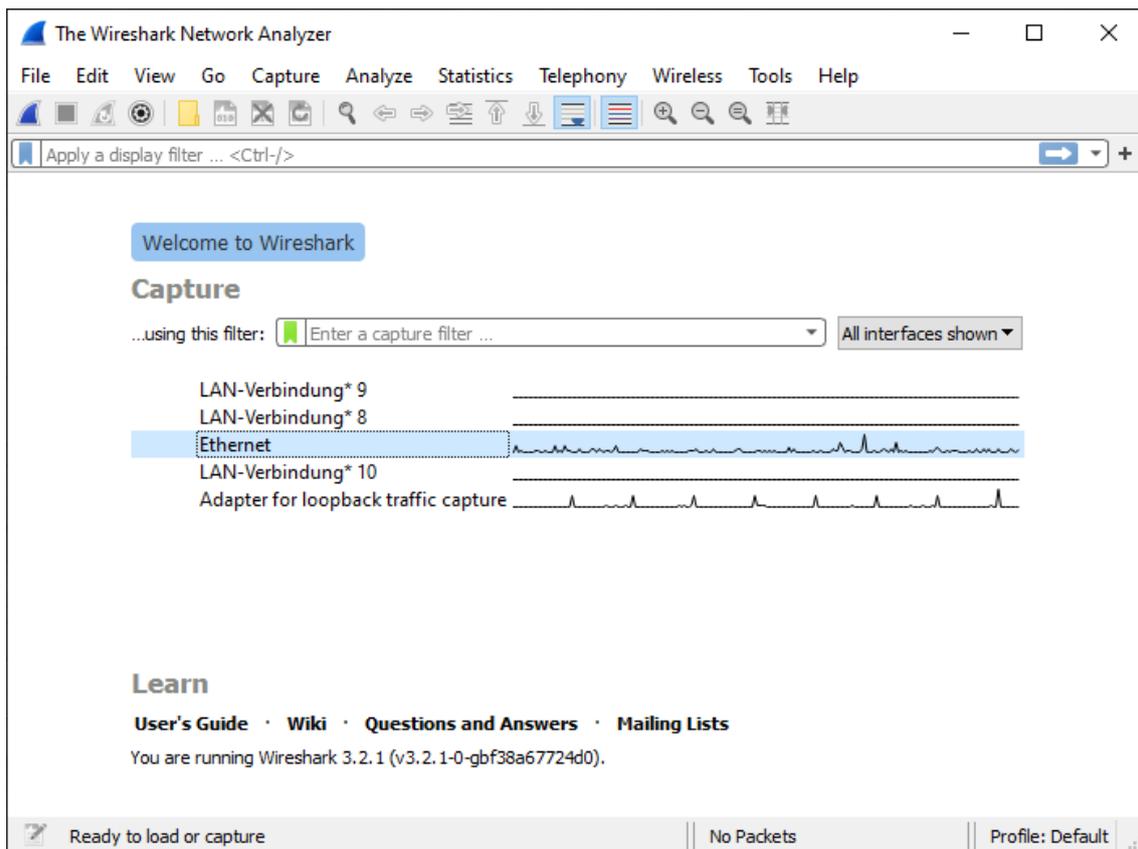


Figure 1. Dialog to select network interface

To begin Wireshark in capture mode, a user double-clicks on one of the displayed network interfaces (Figure 37).

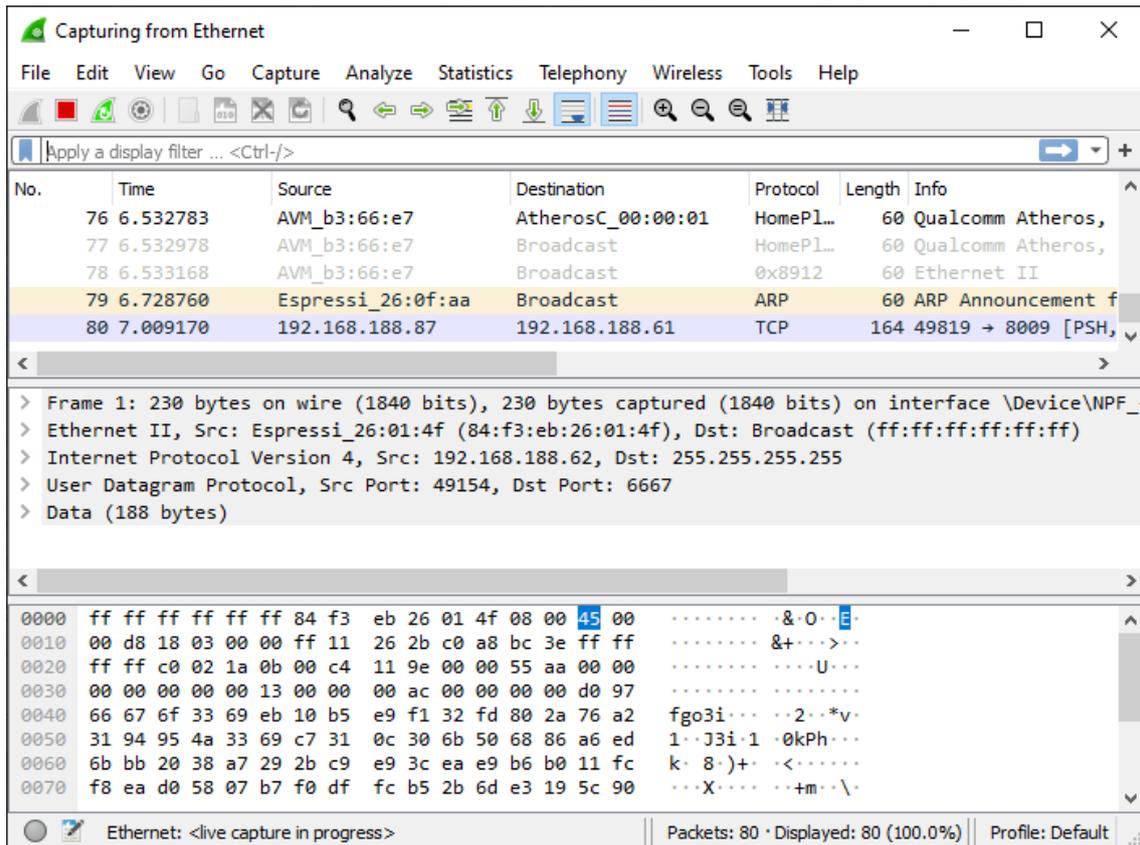


Figure 2. View of Wireshark in capturing mode

Often large amounts of network traffic are present. To focus on a specific address or packet type it is useful to apply a filter by selecting the text field (highlighted in Figure 38).

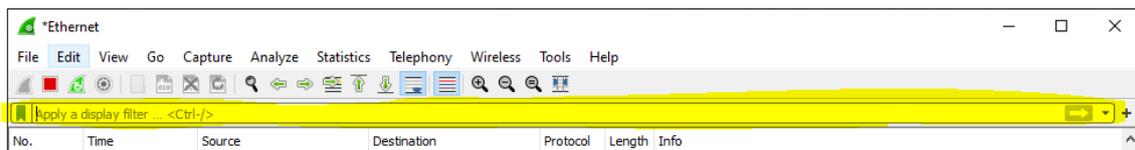


Figure 3. View of text field for filter expression

The syntax to apply a filter for a specific network address is `ip.addr == <IP addr>`. For this example, `ip.addr == 192.168.188.255` is entered, which is the multicast address being used for the DIS simulation in progress. After applying the filter by pressing {Enter}, Wireshark displays all packets with 192.168.188.255 either as source or destination address (Figure 39).

No.	Time	Source	Destination	Protocol	Length	Info
13952	602.346192	192.168.188.87	192.168.188.255	BROWSER	243	Host Announcement IPHONE_2, Workstation, Server, NT Works
17267	729.151565	192.168.188.87	192.168.188.255	DIS	186	PDUType: 1 Entity State, Platform, Land, (1:2:3)
17268	729.151631	192.168.188.87	192.168.188.255	DIS	138	PDUType: 2 Fire
17283	730.259162	192.168.188.87	192.168.188.255	DIS	186	PDUType: 1 Entity State, Platform, Land, (1:2:3)
17284	730.259244	192.168.188.87	192.168.188.255	DIS	138	PDUType: 2 Fire
17289	731.350447	192.168.188.87	192.168.188.255	DIS	186	PDUType: 1 Entity State, Platform, Land, (1:2:3)
17290	731.350532	192.168.188.87	192.168.188.255	DIS	138	PDUType: 2 Fire
17314	732.440880	192.168.188.87	192.168.188.255	DIS	186	PDUType: 1 Entity State, Platform, Land, (1:2:3)
17315	732.440977	192.168.188.87	192.168.188.255	DIS	138	PDUType: 2 Fire
17353	733.540216	192.168.188.87	192.168.188.255	DIS	186	PDUType: 1 Entity State, Platform, Land, (1:2:3)
17354	733.540320	192.168.188.87	192.168.188.255	DIS	138	PDUType: 2 Fire

Figure 4. View of an applied filter for a single IP address

To apply an additional filter for a specific protocol, the name of the protocol must be typed in the text field shown in Figure 38. To filter DIS packets, it is enough to type in “dis” and {Enter}. All protocols must be typed in lower case. Thus the example combined filter is `ip.addr == 192.168.188.255 && dis`.

Since Wireshark parses all DIS PDUs, information within a DIS packet gets displayed in a human-readable form. To analyze a single packet’s information, it must be selected to show the details view. When all nodes are expanded, packet information is displayed as shown in Figure 40.

```

> Frame 17267: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface
> Ethernet II, Src: Micro-St_2c:0d:15 (00:d8:61:2c:0d:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.188.87, Dst: 192.168.188.255
> User Datagram Protocol, Src Port: 3000, Dst Port: 3000
▼ Distributed Interactive Simulation
  > Header
  ▼ Entity State PDU
    ▼ Entity ID
      Entity ID Site: 1
      Entity ID Application: 2
      Entity ID Entity: 3
      Force ID: 0
      Number of Articulation Parameters: 0
    ▼ Entity Type, (1:1:225:1:1:3:0)
      Kind: Platform (1)
      Domain: Land (1)
      Country: United States (225)
      Category / Land: Tank (1)
      Subcategory: 1
      Specific: 3
      Extra: 0
    ▼ Alternative Entity Type, (0:0:0:0:0:0:0)
      Kind: Other (0)
      Domain: Other (0)
      Country: Other (0)
      Category: 0
      Subcategory: 0
      Specific: 0
      Extra: 0
    ▼ Entity Linear Velocity
      X: 0
      Y: 0
      Z: 0
    ▼ Entity Location
      X: -2707488,36777687
      Y: -4353666,73524438
      Z: 3781450,32027544
    ▼ Entity Orientation
      Psi: 0
      Theta: 0
      Phi: 0
      Appearance: 0x00000000
    ▼ Dead Reckoning Parameters
      Dead Reckoning Algorithm: Other (0)
      Dead Reckoning Other Parameters: 00000000000000000000000000000000
    ▼ Entity Linear Acceleration
      Entity Linear Aceleration X: 0
      Entity Linear Aceleration Y: 0
      Entity Linear Aceleration Z: 0
    ▼ Entity Angular Velocity
      Entity Angular Velocity X: 0
      Entity Angular Velocity Y: 0
      Entity Angular Velocity Z: 0
    ▼ Entity Marking
      Entity Character Set: Unused (0)
      Capabilities: 0

```

Figure 5. Details of a single DIS PDU packet parsed by Wireshark

Using AllPduSender.java to send all 72 DIS PDUs to multicast address 239.1.2.3 leads to a capture of all 72 PDUs in Wireshark (Figure 41). Screen capture information can also be copied and saved as a plain-text data file for further processing and analysis.

Source	Destination	Protocol	Length	Info
192.168.188.87	239.1.2.3	DIS	186	PDUType: 1 Entity State, Other, Other, (0:0:0)
192.168.188.87	239.1.2.3	DIS	138	PDUType: 2 Fire
192.168.188.87	239.1.2.3	DIS	146	PDUType: 3 Detonation
192.168.188.87	239.1.2.3	DIS	102	PDUType: 4 Collision
192.168.188.87	239.1.2.3	DIS	70	PDUType: 5 Service Request
192.168.188.87	239.1.2.3	DIS	70	PDUType: 6 Resupply Offer
192.168.188.87	239.1.2.3	DIS	70	PDUType: 7 Resupply Received
192.168.188.87	239.1.2.3	DIS	66	PDUType: 8 Resupply Cancel
192.168.188.87	239.1.2.3	DIS	70	PDUType: 9 Repair Complete
192.168.188.87	239.1.2.3	DIS	70	PDUType: 10 Repair Response
192.168.188.87	239.1.2.3	DIS	70	PDUType: 11 Create Entity
192.168.188.87	239.1.2.3	DIS	70	PDUType: 12 Remove Entity
192.168.188.87	239.1.2.3	DIS	86	PDUType: 13 Start / Resume
192.168.188.87	239.1.2.3	DIS	82	PDUType: 14 Stop / Freeze
192.168.188.87	239.1.2.3	DIS	74	PDUType: 15 Acknowledge
192.168.188.87	239.1.2.3	DIS	82	PDUType: 16 Action Request
192.168.188.87	239.1.2.3	DIS	82	PDUType: 17 Action Response
192.168.188.87	239.1.2.3	DIS	82	PDUType: 18 Data Query
192.168.188.87	239.1.2.3	DIS	82	PDUType: 19 Set Data
192.168.188.87	239.1.2.3	DIS	82	PDUType: 20 Data
192.168.188.87	239.1.2.3	DIS	82	PDUType: 21 Event Report
192.168.188.87	239.1.2.3	DIS	130	PDUType: 22 Comment
192.168.188.87	239.1.2.3	DIS	70	PDUType: 23 Electromagnetic Emission
192.168.188.87	239.1.2.3	DIS	130	PDUType: 24 Designator, CodeName=0
192.168.188.87	239.1.2.3	DIS	149	PDUType: 25 Transmitter, RadioID=0, Transmit State=Off
192.168.188.87	239.1.2.3	DIS	78	PDUType: 26 Signal, RadioID=0, Encoding Type=Unknown
192.168.188.87	239.1.2.3	DIS	78	PDUType: 27 Receiver
192.168.188.87	239.1.2.3	DIS	102	PDUType: 28 IFF, 0-0-0
192.168.188.87	239.1.2.3	DIS	74	PDUType: 29 Underwater Acoustic, Shafts=0, APA=0, Acoustic Emitter=0
192.168.188.87	239.1.2.3	DIS	70	PDUType: 30 Supplemental Emission Entity State
192.168.188.87	239.1.2.3	DIS	78	PDUType: 31 Intercom Signal, RadioID=0, Encoding Type=Unknown
192.168.188.87	239.1.2.3	DIS	82	PDUType: 32 Intercom Control, SourceLineID=0
192.168.188.87	239.1.2.3	DIS	178	PDUType: 33 Aggregate State, (0:0:0),
192.168.188.87	239.1.2.3	DIS	82	PDUType: 34 IsGroupOf
192.168.188.87	239.1.2.3	DIS	82	PDUType: 35 Transfer Ownership
192.168.188.87	239.1.2.3	DIS	94	PDUType: 36 IsPartOf
192.168.188.87	239.1.2.3	DIS	114	PDUType: 37 Minefield State
192.168.188.87	239.1.2.3	DIS	82	PDUType: 38 Minefield Query
192.168.188.87	239.1.2.3	DIS	86	PDUType: 39 Minefield Data
192.168.188.87	239.1.2.3	DIS	68	PDUType: 40 Minefield Response NACK
192.168.188.87	239.1.2.3	DIS	74	PDUType: 41 Environmental Process
192.168.188.87	239.1.2.3	DIS	106	PDUType: 42 Gridded Data
192.168.188.87	239.1.2.3	DIS	133	PDUType: 43 Point Object State
192.168.188.87	239.1.2.3	DIS	82	PDUType: 44 Linear Object State
192.168.188.87	239.1.2.3	DIS	91	PDUType: 45 Areal Object State
192.168.188.87	239.1.2.3	DIS	98	PDUType: 46 TSPI
192.168.188.87	239.1.2.3	DIS	111	PDUType: 47 Appearance
192.168.188.87	239.1.2.3	DIS	61	PDUType: 48 Articulated Parts
192.168.188.87	239.1.2.3	DIS	111	PDUType: 49 LE Fire
192.168.188.87	239.1.2.3	DIS	123	PDUType: 50 LE Detonation
192.168.188.87	239.1.2.3	DIS	74	PDUType: 51 Create Entity-R
192.168.188.87	239.1.2.3	DIS	74	PDUType: 52 Remove Entity-R
192.168.188.87	239.1.2.3	DIS	90	PDUType: 53 Start / Resume-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 54 Stop / Freeze-R
192.168.188.87	239.1.2.3	DIS	74	PDUType: 55 Acknowledge-R
192.168.188.87	239.1.2.3	DIS	86	PDUType: 56 Action Request-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 57 Action Response-R
192.168.188.87	239.1.2.3	DIS	86	PDUType: 58 Data Query-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 59 Set Data-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 60 Data-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 61 Event Report-R
192.168.188.87	239.1.2.3	DIS	74	PDUType: 62 Comment-R
192.168.188.87	239.1.2.3	DIS	78	PDUType: 63 Record-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 64 Set Record-R
192.168.188.87	239.1.2.3	DIS	82	PDUType: 65 Record Query-R
192.168.188.87	239.1.2.3	DIS	142	PDUType: 66 Collision Elastic
192.168.188.87	239.1.2.3	DIS	114	PDUType: 67 Entity State Update, (0:0:0)
192.168.188.87	239.1.2.3	DIS	130	PDUType: 68 Directed Energy Fire
192.168.188.87	239.1.2.3	DIS	66	PDUType: 69 Entity Damage Status
192.168.188.87	239.1.2.3	DIS	98	PDUType: 70 Info Operations Action
192.168.188.87	239.1.2.3	DIS	82	PDUType: 71 Info Operations Report
192.168.188.87	239.1.2.3	DIS	74	PDUType: 72 Attribute

Figure 6. All 72 IEEE DIS PDU types captured with Wireshark

Reference:

WireShark. (n.d.). *Go Deep*. Retrieved January 28, 2020, from <https://www.wireshark.org/>