

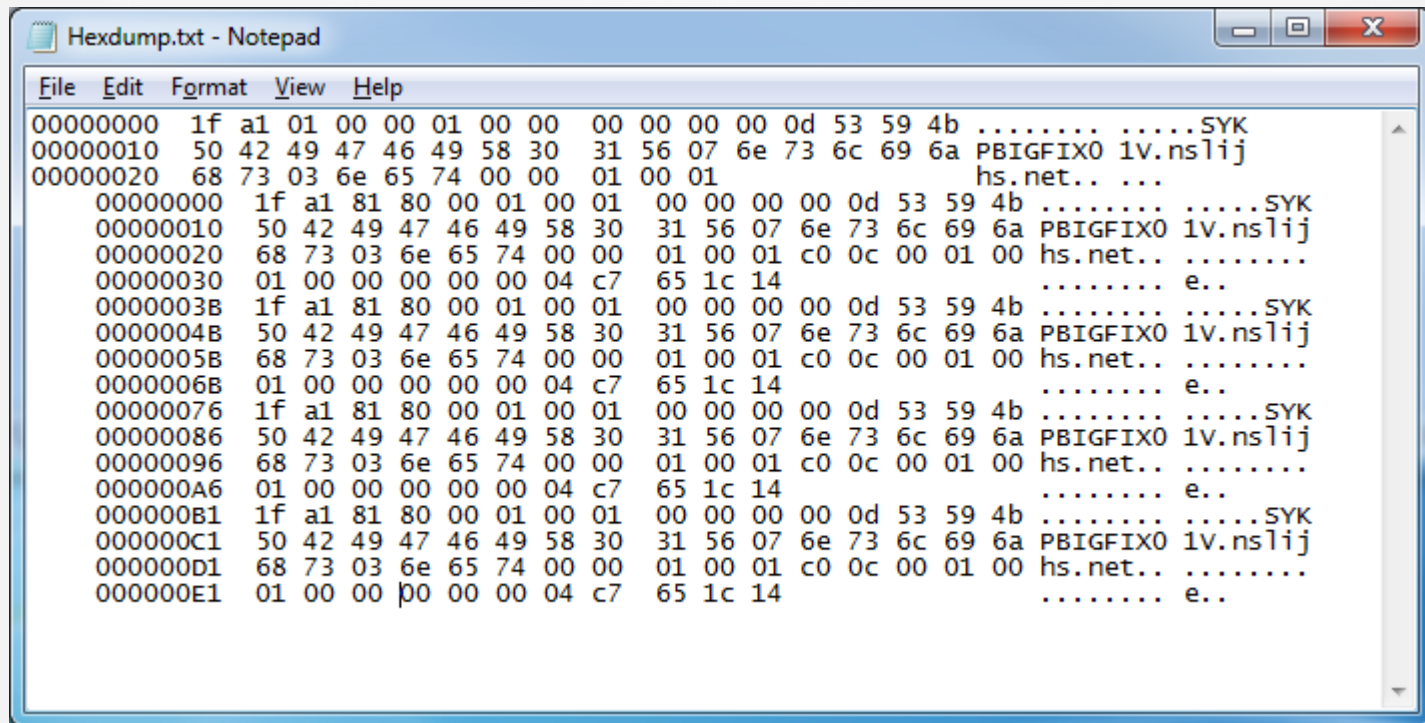


Importing Data

Importing Data

- » **Using Wireshark to import data**
- » **Importing Hex**
 - Import Hex Dump
- » **Why is this useful?**
 - Create a viewable conversation
 - Packet- or frame-based communication viewable in the Capture window

Importing Data



```
Hexdump.txt - Notepad
File Edit Format View Help
00000000 1f a1 01 00 00 01 00 00 00 00 00 0d 53 59 4b .....SYK
00000010 50 42 49 47 46 49 58 30 31 56 07 6e 73 6c 69 6a PBIGFIX0 1v.nslj
00000020 68 73 03 6e 65 74 00 00 01 00 01
hs.net.. ...
00000000 1f a1 81 80 00 01 00 01 00 00 00 0d 53 59 4b .....SYK
00000010 50 42 49 47 46 49 58 30 31 56 07 6e 73 6c 69 6a PBIGFIX0 1v.nslj
00000020 68 73 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 hs.net.. .....
00000030 01 00 00 00 00 00 04 c7 65 1c 14
..... e..
0000003B 1f a1 81 80 00 01 00 01 00 00 00 0d 53 59 4b .....SYK
0000004B 50 42 49 47 46 49 58 30 31 56 07 6e 73 6c 69 6a PBIGFIX0 1v.nslj
0000005B 68 73 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 hs.net.. .....
0000006B 01 00 00 00 00 00 04 c7 65 1c 14
..... e..
00000076 1f a1 81 80 00 01 00 01 00 00 00 0d 53 59 4b .....SYK
00000086 50 42 49 47 46 49 58 30 31 56 07 6e 73 6c 69 6a PBIGFIX0 1v.nslj
00000096 68 73 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 hs.net.. .....
000000A6 01 00 00 00 00 00 04 c7 65 1c 14
..... e..
000000B1 1f a1 81 80 00 01 00 01 00 00 00 0d 53 59 4b .....SYK
000000C1 50 42 49 47 46 49 58 30 31 56 07 6e 73 6c 69 6a PBIGFIX0 1v.nslj
000000D1 68 73 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 hs.net.. .....
000000E1 01 00 00 00 00 00 04 c7 65 1c 14
..... e..
```

Importing Data

- » **Setting options**
- » **Import dialog box**
 - Format
 - Encapsulation
 - Offsets
 - Others
- » **Recreate the conversation**
 - Rebuild in the Capture window

Importing Data

No.	Time	Source	Destination	Protocol	Expert	Length	Info
1	0.000000000	00:00:00_00:00:00	1f:a1:01:00:00:01	0x0d53		43	Ethernet II
2	0.000001000	EquipTra_00:00:00	1f:a1:81:80:00:01	0x0d53		236	Ethernet II

Frame 2: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface 0

- Interface id: 0
- Packet flags: 0x00000000
- Encapsulation type: Ethernet (1)
- Arrival Time: May 27, 2014 11:38:45.000001000 Eastern Daylight Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1401205125.000001000 seconds
- [Time delta from previous captured frame: 0.000001000 seconds]
- [Time delta from previous displayed frame: 0.000001000 seconds]
- [Time since reference or first frame: 0.000001000 seconds]
- Frame Number: 2
- Frame Length: 236 bytes (1888 bits)
- Capture Length: 236 bytes (1888 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:data]
- [Coloring Rule Name: Broadcast]
- [Coloring Rule String: eth[0] & 1]

Ethernet II, Src: EquipTra_00:00:00 (00:01:00:00:00:00), Dst: 1f:a1:81:80:00:01 (1f:a1:81:80:00:01)

- Destination: 1f:a1:81:80:00:01 (1f:a1:81:80:00:01)
- Source: EquipTra_00:00:00 (00:01:00:00:00:00)
- Type: Unknown (0x0d53)

Data (222 bytes)

Data: 594b50424947464958303156076e736c696a6873036e6574...

[Length: 222]

Questions?