**From:** Acosta, Tony (AS)   
**Sent:** Thursday, February 28, 2013 11:51 AM  
**To:** Cento, Steven J (AS)  
**Subject:** RE: I have the 2 DVDs (what I see on them, and what format looks like...)

Yes, the two DVDs are identical, and you figured out the code.  Keep one for yourself and give the other one to them.  Copy if you like, they are unclass

**From:** Cento, Steven J (AS)   
**Sent:** Wednesday, February 27, 2013 5:41 PM  
**To:** Acosta, Tony (AS)  
**Subject:** RE: I have the 2 DVDs (what I see on them, and what format looks like...)

Tony,

I think I figured some of it out per your most recent email note below suggesting that I “…look at the big files and see if you can figure out one of them, probably the excel spreadsheet”.

The 2 DVDs appear to be duplicate copies of one another (note I still need to 100% confirm that, but it appears so on quick check).

On each DVD…

The 1st file “TestNetworkData.csv” (where CSV= Comma Separated Value, but is blank field delimited instead for Excel equivalence) contains the network test data with named column fields (as is typical of all ASCII CSV data files).  The 6 column fields are sequential record “No., “Time” as real-valued incremental seconds since midnight to 6 decimal places, “Source” (either network ID or host IP address) sending the data, “Destination” (either network ID or host IP address) receiving the data, “Protocol” type (e.g., STP or TCP or FTP-DATA, or etc., etc.), and “Info” about what is being passed (e.g., # bytes for FTP, other network parameter info like Mask and Port # for STP, and ACK, Seq, etc. for TCP, etc., etc.).

I expanded the column widths out, so I could see all data in all fields as I scroll down thru the file. I copied the reformatted .csv file to .xls - that didn’t work since old Excel has much smaller interactive row record I/O limits,  but then copied to latest .xlsx and that worked fine – entire reformatted .csv copied and now more readable since columns fully expanded.

I then opened your last file “acosta\_testdata2.txt” and compared it to the reformatted 1st file TestNetworkData.xlsx” and saw everything *almost* corresponds record by record throughout, *except* there is the following additional info in “acosta\_testdata2.txt”:

1. The message data in the CSV “Info” fields that start with “Root=”<number> has that <number> split up into a common numeric baseline value of 32768 = 215,  concatenated with additional “/” delimiter and numeric offset value from baseline, so when added together those always equal the “Root=” numeric value in the corresponding Excel or CSV file record; and
2. The text file also contains additional network data attributes interleaved for each record that do not appear in “TestNetworkData.csv”, and some of those additional network and/or host communications attributes have more detailed information as I scroll down, that looks important, like number of bytes sent on wire & captured, additional descriptive protocol info, etc.

So between those two key files interleaved, it looks like almost everything we’d need is captured.

There are also multiple.avi “video” files that contain some nice animations of the network nodes and links between nodes as data is being transferred between, both for all traffic, normal traffic, and anomalous (network attack) traffic situations.  The VLC Media player that I downloaded & installed last week to view the compressed MPEG4 video of 30-Jan DARPA I2O ICAT Proposer’s Day, also works fine for those .avi files.

What I don’t yet see in any of the DVD files is the actual network data info being transferred, captured in record form. e.g., the actual binary bit stream and/or ASCII character byte string equivalent packet data that’s being transferred in each packet for the specified # of bytes sent & received.  There’s descriptive network/host communications attribution on each packet being transferred, but not the actual packet data itself, just supporting info on the packet data that’s being transferred.  But maybe the latter is all that’s contained in this Challenge Network test data set?  If so, is that enough?  (i.e., do Cyber detectives typically only use the network/host and packet descriptive info and not the raw packet data itself, because latter looks normal even during an intrusion/attack but they can see abnormal signs in the former?).

There are also several other Microsoft Access DB files (or links to files) on the DVD containing network node graphs, etc.  But I can’t easily read those files from my laptop or desktop (yet).

--Steve

**From:** Acosta, Tony (AS)   
**Sent:** Wednesday, February 27, 2013 12:05 PM  
**To:** Cento, Steven J (AS)  
**Subject:** RE: I have the 2 DVDs

I won’t be back in LA until Saturday; look at the big files and see if you can figure out one of them, probably the excel spreadsheet.

**From:** Cento, Steven J (AS)   
**Sent:** Wednesday, February 27, 2013 7:57 AM  
**To:** Acosta, Tony (AS)  
**Subject:** RE: I have the 2 DVDs

OK good thanks for the heads up.  If/when you find the decoder file in your archives, you can email it to me as an attachment, thanks.  I’ll still review the Challenge Network files I have, but I’ll hold a bit on sending a copy to NGIS Donald Steiner until we have the decoder file for him to use so he knows how to read the data.   I may still have some questions about other aspects of the files I have, I will know more on that later today.

**From:** Acosta, Tony (AS)   
**Sent:** Wednesday, February 27, 2013 7:35 AM  
**To:** Cento, Steven J (AS)  
**Subject:** RE: I have the 2 DVDs

I remember it had a funky format, and I have the decoder ring in a file in my archives.

**From:** Cento, Steven J (AS)   
**Sent:** Tuesday, February 26, 2013 8:08 PM  
**To:** Acosta, Tony (AS)  
**Subject:** I have the 2 DVDs

I have the 2 DVDs that you copied for me, that contain your Challenge network test data – I picked them up from Plant 5 today.  After I finish looking at the files/data, I may have some questions for you, before I send the data out to NGIS Donald Steiner for RADISH testing.

**From:** Acosta, Tony (AS)   
**Sent:** Tuesday, February 19, 2013 3:33 PM  
**To:** Cento, Steven J (AS)  
**Subject:** RE: DVD from Tony Acosta

This is a network that has undergone a change in posture, a “state change”.  No virus.