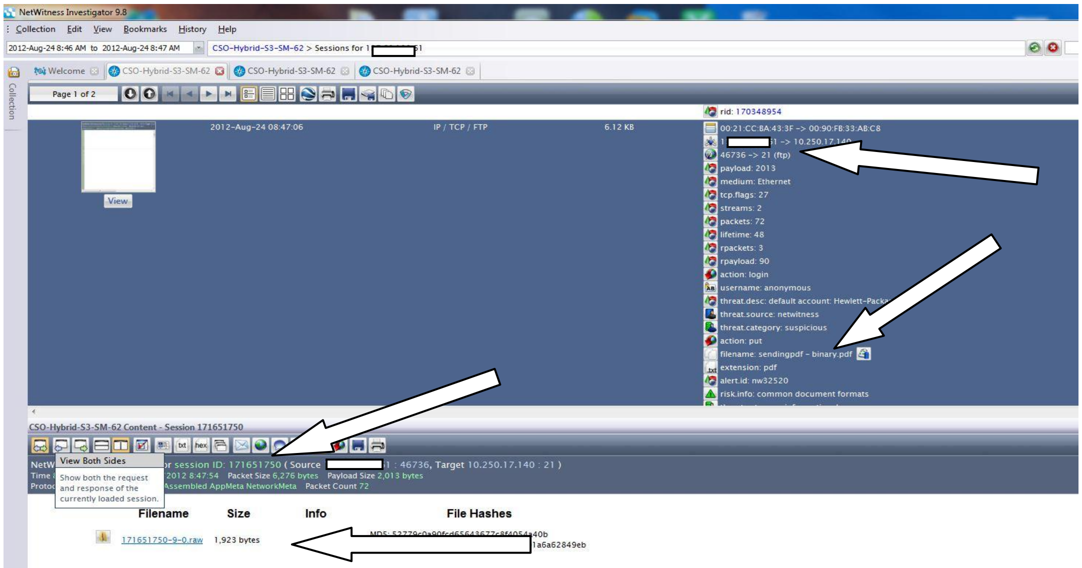
Recovering a file sent over Port 21 FTP

While reviewing activity in Investigator in **Hybrid View** we see a user sent a file over Port 21 (FTP) that we want to take a closer look at and view the actual file. In our example a user sent a file named '**sendingpdf – binary.pdf**' in **Session ID 171651750**.

NOTE: the filename below in the white area was changed to **<Session ID>.raw.Ext** This will be the filename we recover when we download the file.


NetWitness Investigator 9.8
Collection Edit View Bookmarks History Help
2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM
CSO-Hybrid-S3-SM-62 > Sessions for [redacted]
Welcome
CSO-Hybrid-S3-SM-62
CSO-Hybrid-S3-SM-62
CSO-Hybrid-S3-SM-62
Collection
Page 1 of 2
View
txt
hex
View Both Sides

2012-Aug-24 08:47:06 IP / TCP / FTP 6.12 KB

```
rid: 170348954
00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8
[redacted] -> 10.250.17.140
46736 -> 21 (ftp)
payload: 2013
medium: Ethernet
tcp.flags: 27
streams: 2
packets: 72
lifetime: 48
rpackets: 3
rpayload: 90
action: login
username: anonymous
threat.desc: default account: Hewlett-Packa
threat.source: netwitness
threat.category: suspicious
action: put
filename: sendingpdf – binary.pdf
extension: pdf
alert.id: nw32520
risk.info: common document formats
```

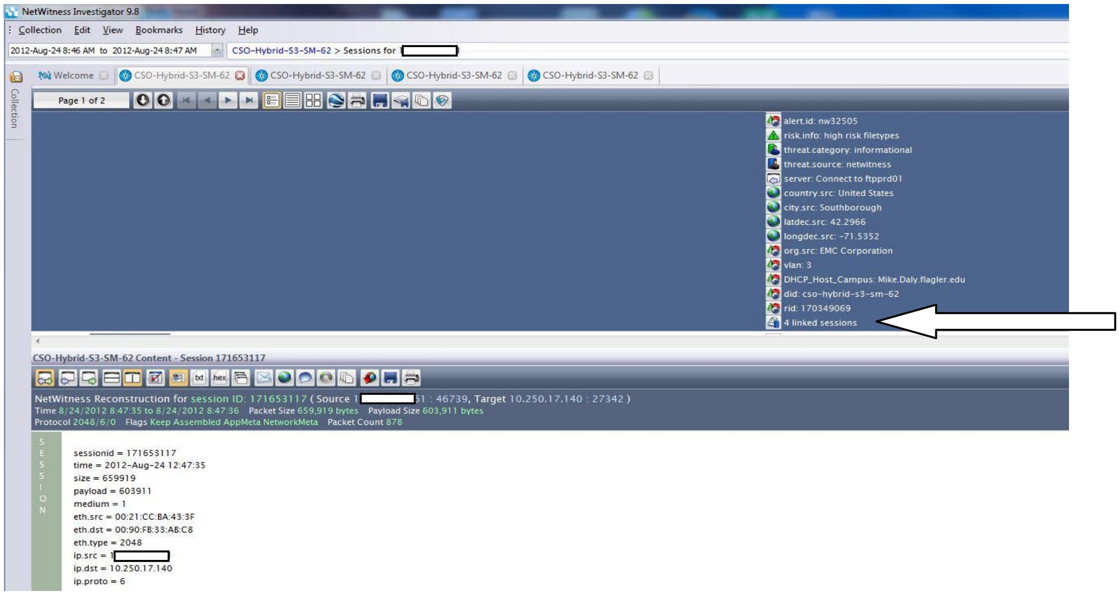
CSO-Hybrid-S3-SM-62 Content - Session 171651750

Show both the request and response of the currently loaded session.

NetW... session ID: 171651750 (Source [redacted] : 46736, Target 10.250.17.140 : 21)
Time ... 2012 8:47:54 Packet Size 6,276 bytes Payload Size 2,013 bytes
Protoc... Assembled AppMeta NetworkMeta Packet Count 72

Filename	Size	Info	File Hashes
171651750-9-0.raw	1,923 bytes		MD5: 52779c0a90fcd65643677c8f4054a40b 1a6a62849eb

The actual file was sent on other ports under another Session ID to find this information Select 'Linked Sessions' at the bottom. In this example there are 4 Linked Sessions.


NetWitness Investigator 9.8
Collection Edit View Bookmarks History Help
2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM
CSO-Hybrid-S3-SM-62 > Sessions for [redacted]
Welcome
CSO-Hybrid-S3-SM-62
CSO-Hybrid-S3-SM-62
CSO-Hybrid-S3-SM-62
CSO-Hybrid-S3-SM-62
Collection
Page 1 of 2
txt
hex
SESSION

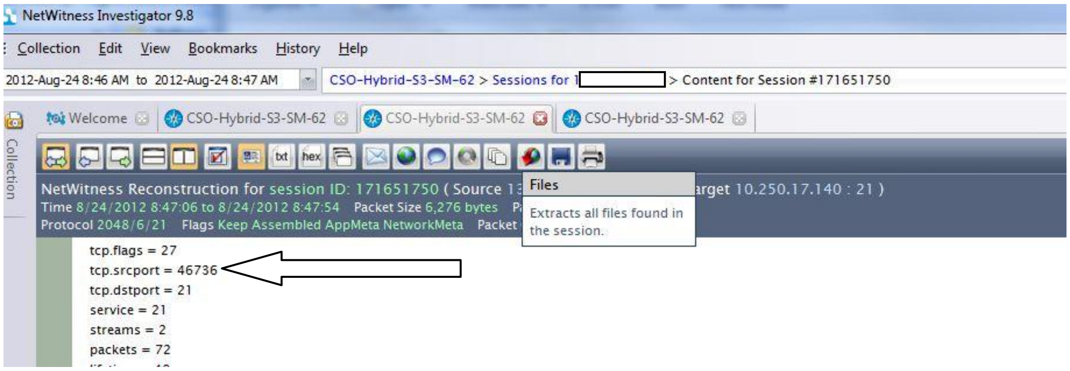
```
alert.id: nw32505
risk.info: high risk filetypes
threat.category: informational
threat.source: netwitness
server: Connect to ftpprd01
country.src: United States
city.src: Southborough
latdec.src: 42.2966
longdec.src: -71.5352
org.src: EMC Corporation
vlan: 3
DHCP_Host_Campus: Mike.Daly.flagler.edu
did: cso-hybrid-s3-sm-62
rid: 170349069
4 linked sessions
```

CSO-Hybrid-S3-SM-62 Content - Session 171653117

NetWitness Reconstruction for session ID: 171653117 (Source [redacted] : 46739, Target 10.250.17.140 : 27342)
Time 8/24/2012 8:47:35 to 8/24/2012 8:47:36 Packet Size 659,919 bytes Payload Size 603,911 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 878

```
sessionid = 171653117
time = 2012-Aug-24 12:47:35
size = 659919
payload = 603911
medium = 1
eth.src = 00:21:CC:BA:43:3F
eth.dst = 00:90:FB:33:AB:C8
eth.type = 2048
ip.src = [redacted]
ip.dst = 10.250.17.140
ip.proto = 6
```

When you select the linked sessions it opens 2 tabs first tab shows the Command Session still using **Session ID 171651750** indicating **tcp.dstport 21** will use **tcp.srcport 46736** to transmit the file.



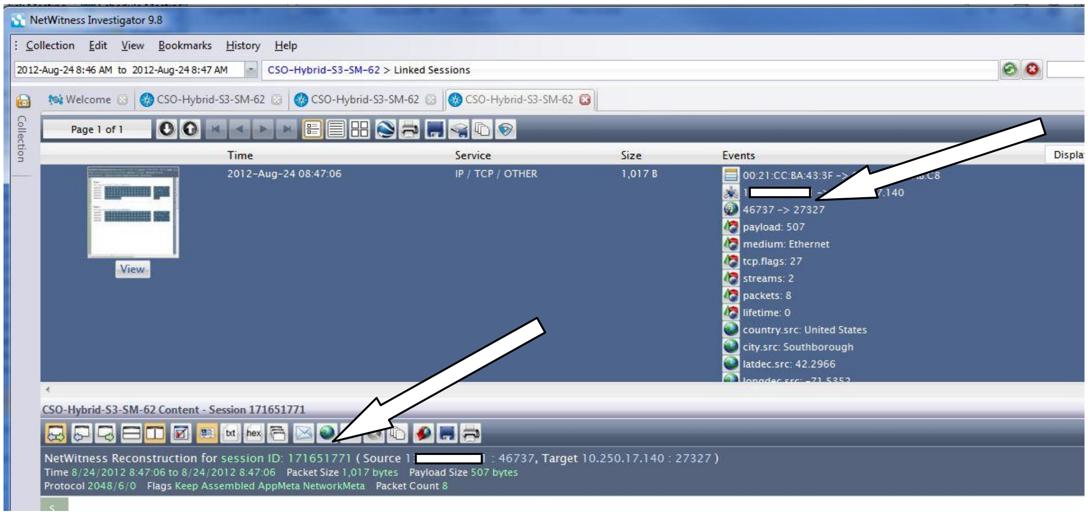
2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM

CSO-Hybrid-S3-SM-62 > Sessions for 1[redacted] > Content for Session #171651750

Extracts all files found in the session.

```
NetWitness Reconstruction for session ID: 171651750 ( Source 13 ... arget 10.250.17.140 : 21 )
Time 8/24/2012 8:47:06 to 8/24/2012 8:47:54   Packet Size 6,276 bytes   Pa
Protocol 2048/6/21   Flags Keep Assembled AppMeta NetworkMeta   Packet
tcp.flags = 27
tcp.srcport = 46736
tcp.dstport = 21
service = 21
streams = 2
packets = 72
```

The 2nd tab shows the data being transmitted from **port 46737** to **Port 27327**
Note the new **Session ID of 171653117**



2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM

CSO-Hybrid-S3-SM-62 > Linked Sessions

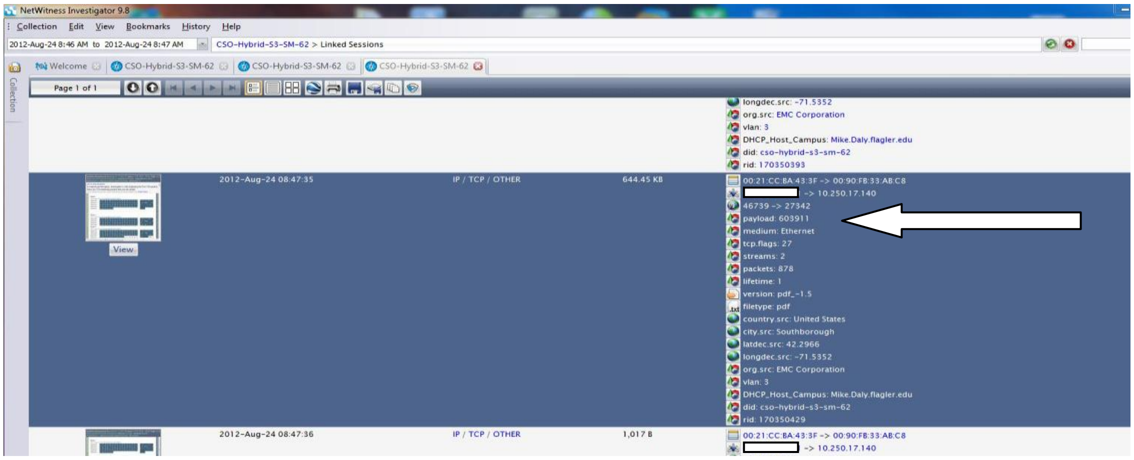
Time	Service	Size	Events
2012-Aug-24 08:47:06	IP / TCP / OTHER	1,017 B	00:21:CC:BA:43:3F -> ...:C8 1[redacted] -> ...7.140 46737 -> 27327 payload: 507 medium: Ethernet tcp.flags: 27 streams: 2 packets: 8 lifetime: 0 country.src: United States city.src: Southborough latdec.src: 42.2966 longdec.src: -71.5352

CSO-Hybrid-S3-SM-62 Content - Session 171651771

```
NetWitness Reconstruction for session ID: 171651771 ( Source 1[redacted]1 : 46737, Target 10.250.17.140 : 27327 )
Time 8/24/2012 8:47:06 to 8/24/2012 8:47:06   Packet Size 1,017 bytes   Payload Size 507 bytes
Protocol 2048/6/0   Flags Keep Assembled AppMeta NetworkMeta   Packet Count 8
```

Select the session with a sizable payload in this example the **payload is 603911** while the other 3 linked sessions one session had a payload of 0 and two had payload sizes of 507 each.

NOTE: Sessions are created each time you send a command to FTP e.g. cd, ls, dir, put etc, will all create a unique Session ID which is why sending one file via FTP may create several sessions.



NetWitness Investigator 9.8

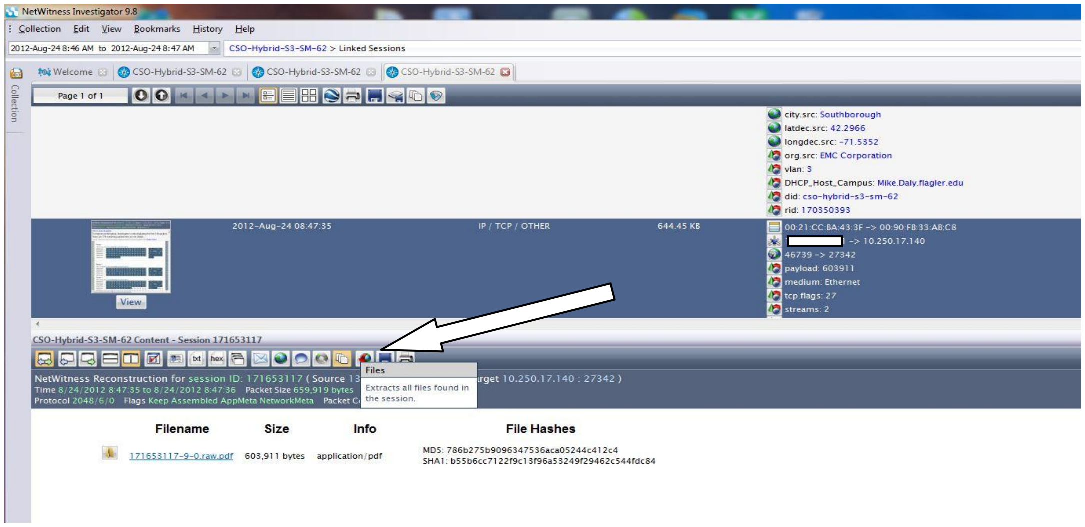
2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM CSO-Hybrid-S3-SM-62 > Linked Sessions

```
longdec.src: -71.5352
org.src: EMC Corporation
vlan: 3
DHCP_Host_Campus: Mike.Daly.flagler.edu
did: cso-hybrid-s3-sm-62
rid: 170350393

2012-Aug-24 08:47:35    IP / TCP / OTHER    644.45 KB
00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8
[redacted] -> 10.250.17.140
46739 -> 27342
payload: 603911
medium: Ethernet
tcp.flags: 27
streams: 2
packets: 878
lifetime: 1
version: pdf_-1.5
filetype: pdf
country.src: United States
city.src: Southborough
latdec.src: 42.2966
longdec.src: -71.5352
org.src: EMC Corporation
vlan: 3
DHCP_Host_Campus: Mike.Daly.flagler.edu
did: cso-hybrid-s3-sm-62
rid: 170350429

2012-Aug-24 08:47:36    IP / TCP / OTHER    1,017 B
00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8
[redacted] -> 10.250.17.140
```

Select Files tab which reveals a pdf file of 603,911 bytes.



NetWitness Investigator 9.8

2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM CSO-Hybrid-S3-SM-62 > Linked Sessions

```
city.src: Southborough
latdec.src: 42.2966
longdec.src: -71.5352
org.src: EMC Corporation
vlan: 3
DHCP_Host_Campus: Mike.Daly.flagler.edu
did: cso-hybrid-s3-sm-62
rid: 170350393

2012-Aug-24 08:47:35    IP / TCP / OTHER    644.45 KB
00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8
[redacted] -> 10.250.17.140
46739 -> 27342
payload: 603911
medium: Ethernet
tcp.flags: 27
streams: 2
```

CSO-Hybrid-S3-SM-62 Content - Session 171653117

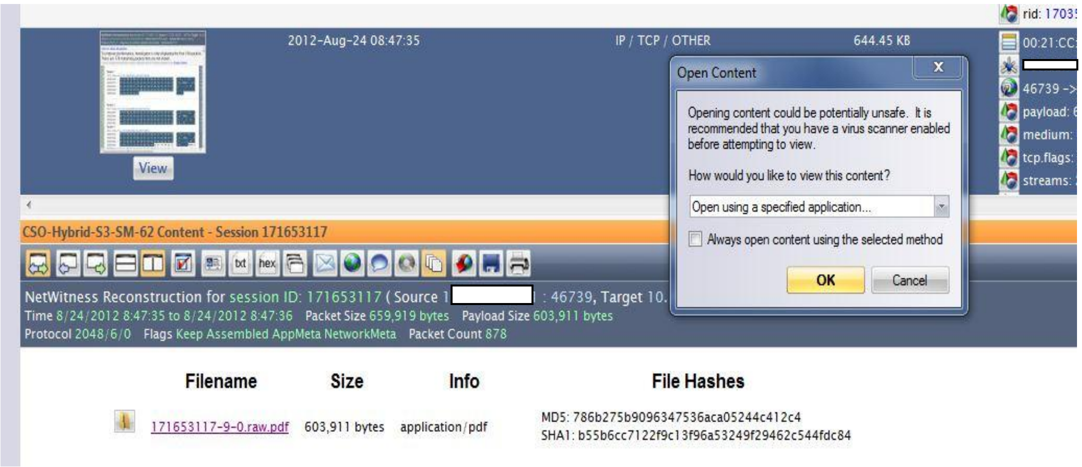
Files

Extracts all files found in the session.

NetWitness Reconstruction for session ID: 171653117 (Source 13 … rget 10.250.17.140 : 27342)
Time 8/24/2012 8:47:35 to 8/24/2012 8:47:36 Packet Size 659,919 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet C

Filename	Size	Info	File Hashes
171653117-9-0.raw.pdf	603,911 bytes	application/pdf	MD5: 786b275b9096347536aca05244c412c4 SHA1: b55b6cc7122f9c13f96a53249f29462c544fdc84

If you select the file it opens a content window chose either a location to save it or an application to open it. In this example we choose 'Open using a specific application' and **Select OK**.



```
2012-Aug-24 08:47:35    IP / TCP / OTHER    644.45 KB
rid: 1703
00:21:CC
[redacted]
46739 ->
payload:
medium:
tcp.flags:
streams:
```

CSO-Hybrid-S3-SM-62 Content - Session 171653117

Open Content

Opening content could be potentially unsafe. It is recommended that you have a virus scanner enabled before attempting to view.

How would you like to view this content?

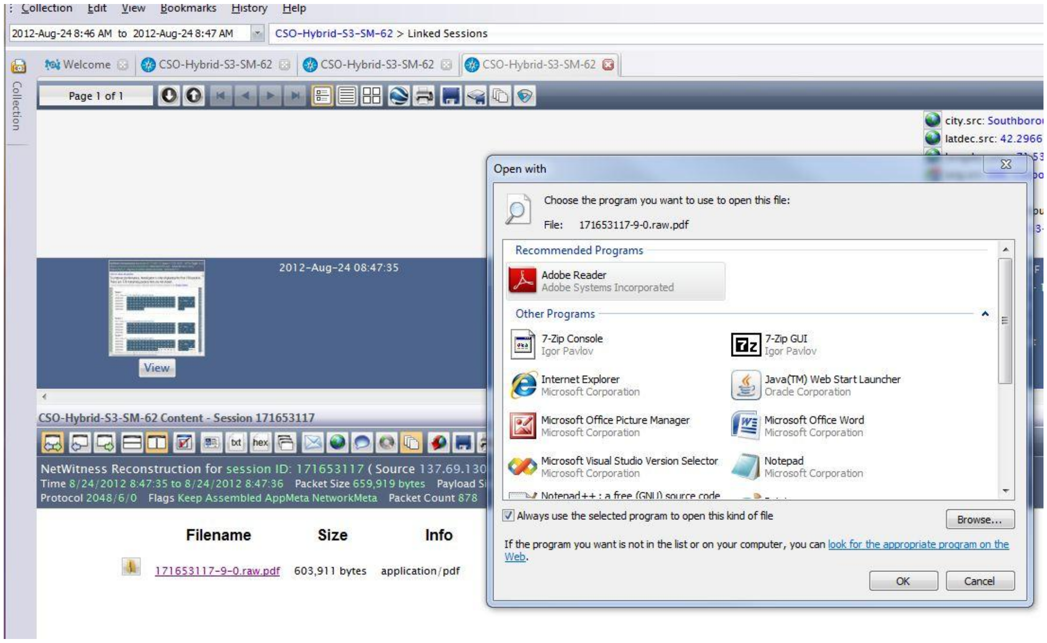
Open using a specified application...

□ Always open content using the selected method

NetWitness Reconstruction for session ID: 171653117 (Source 1 [redacted] : 46739, Target 10.
Time 8/24/2012 8:47:35 to 8/24/2012 8:47:36 Packet Size 659,919 bytes Payload Size 603,911 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 878

Filename	Size	Info	File Hashes
171653117-9-0.raw.pdf	603,911 bytes	application/pdf	MD5: 786b275b9096347536aca05244c412c4 SHA1: b55b6cc7122f9c13f96a53249f29462c544fdc84

Since we see the file extension of .pdf in my example we chose Adobe Reader and **Select OK**.



CSO-Hybrid-S3-SM-62 Content - Session 171653117

NetWitness Reconstruction for session ID: 171653117 (Source 137.69.130
Time 8/24/2012 8:47:35 to 8/24/2012 8:47:36 Packet Size 659,919 bytes Payload S
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 878

Filename	Size	Info
171653117-9-0.raw.pdf	603,911 bytes	application/pdf

Open with

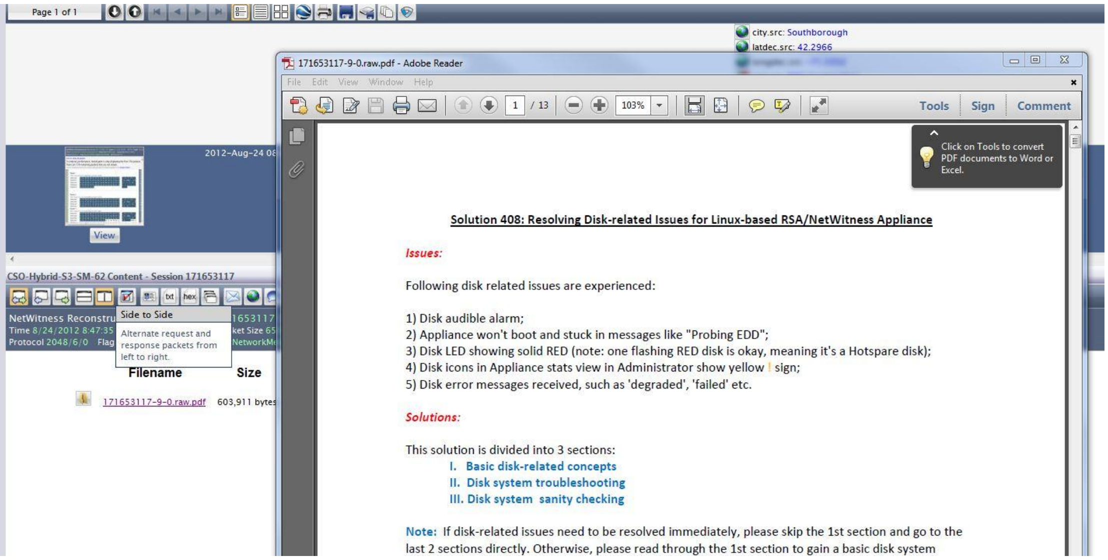
Choose the program you want to use to open this file:

File: 171653117-9-0.raw.pdf

☑ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.

The pdf file is recovered.


Page 1 of 1
city.src: Southborough
latdec.src: 42.2966
2012-Aug-24 08
View
Side to Side
Alternate request and response packets from left to right.
171653117-9-0.raw.pdf - Adobe Reader
File Edit View Window Help
1 / 13
103%
Tools
Sign
Comment
Click on Tools to convert PDF documents to Word or Excel.

CSO-Hybrid-S3-SM-62 Content - Session 171653117

Filename	Size
171653117-9-0.raw.pdf	603,911 bytes

Solution 408: Resolving Disk-related Issues for Linux-based RSA/NetWitness Appliance

Issues:

Following disk related issues are experienced:

1) Disk audible alarm;
2) Appliance won't boot and stuck in messages like "Probing EDD";
3) Disk LED showing solid RED (note: one flashing RED disk is okay, meaning it's a Hotspare disk);
4) Disk icons in Appliance stats view in Administrator show yellow ! sign;
5) Disk error messages received, such as 'degraded', 'failed' etc.

Solutions:

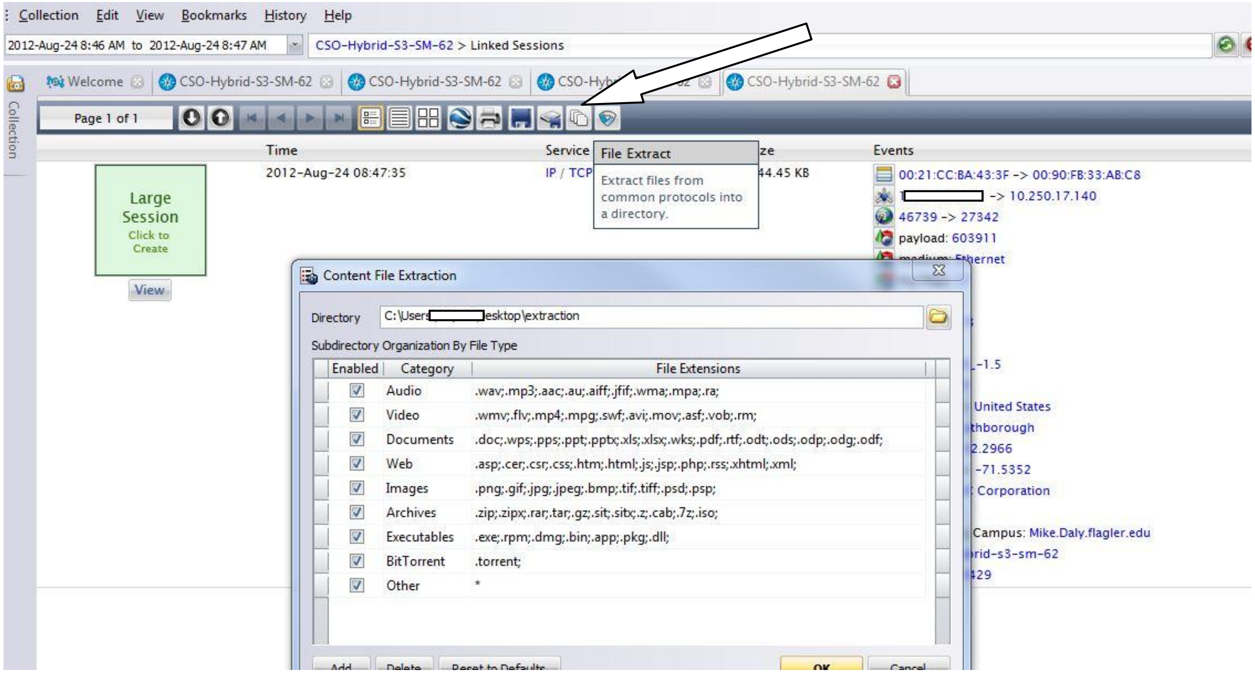
This solution is divided into 3 sections:

I. Basic disk-related concepts
II. Disk system troubleshooting
III. Disk system sanity checking

Note: If disk-related issues need to be resolved immediately, please skip the 1st section and go to the last 2 sections directly. Otherwise, please read through the 1st section to gain a basic disk system

Alternate Method

Alternatively instead of selecting the file to open you can **Select File Extract** which opens a Content File Extraction Window.



2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM

File Extract
Extract files from common protocols into a directory.

Time	Service	ze	Events
2012-Aug-24 08:47:35	IP / TCP	44.45 KB	00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8 [redacted] -> 10.250.17.140 46739 -> 27342 payload: 603911 medium: Ethernet

Content File Extraction

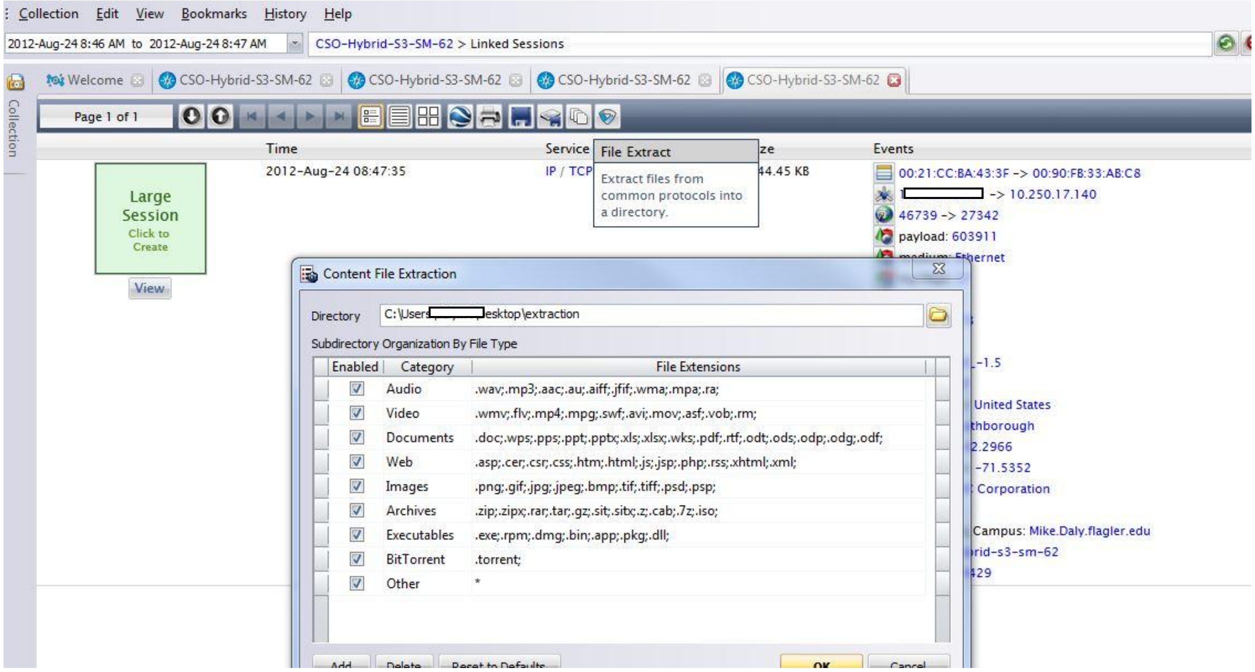
Directory: C:\Users[redacted]esktop\extraction

Subdirectory Organization By File Type

Enabled	Category	File Extensions
☑	Audio	.wav;.mp3;.aac;.au;.aiff;.jfif;.wma;.mpa;.ra;
☑	Video	.wmv;.flv;.mp4;.mpg;.swf;.avi;.mov;.asf;.vob;.rm;
☑	Documents	.doc;.wps;.pps;.ppt;.pptx;.xls;.xlsx;.wks;.pdf;.rtf;.odt;.ods;.odp;.odg;.odf;
☑	Web	.asp;.cer;.csr;.css;.htm;.html;.js;.jsp;.php;.rss;.xhtml;.xml;
☑	Images	.png;.gif;.jpg;.jpeg;.bmp;.tif;.tiff;.psd;.psp;
☑	Archives	.zip;.zipx;.rar;.tar;.gz;.sit;.sitx;.z;.cab;.7z;.iso;
☑	Executables	.exe;.rpm;.dmg;.bin;.app;.pkg;.dll;
☑	BitTorrent	.torrent;
☑	Other	*

-1.5
United States
thborough
2.2966
-71.5352
Corporation
Campus: Mike.Daly.flagler.edu
rid-s3-sm-62
29

Leave defaults checked and **Select Ok** and chose a destination to download the file too.



2012-Aug-24 8:46 AM to 2012-Aug-24 8:47 AM

File Extract
Extract files from common protocols into a directory.

Time	Service	ze	Events
2012-Aug-24 08:47:35	IP / TCP	44.45 KB	00:21:CC:BA:43:3F -> 00:90:FB:33:AB:C8 [redacted] -> 10.250.17.140 46739 -> 27342 payload: 603911 medium: Ethernet

Content File Extraction

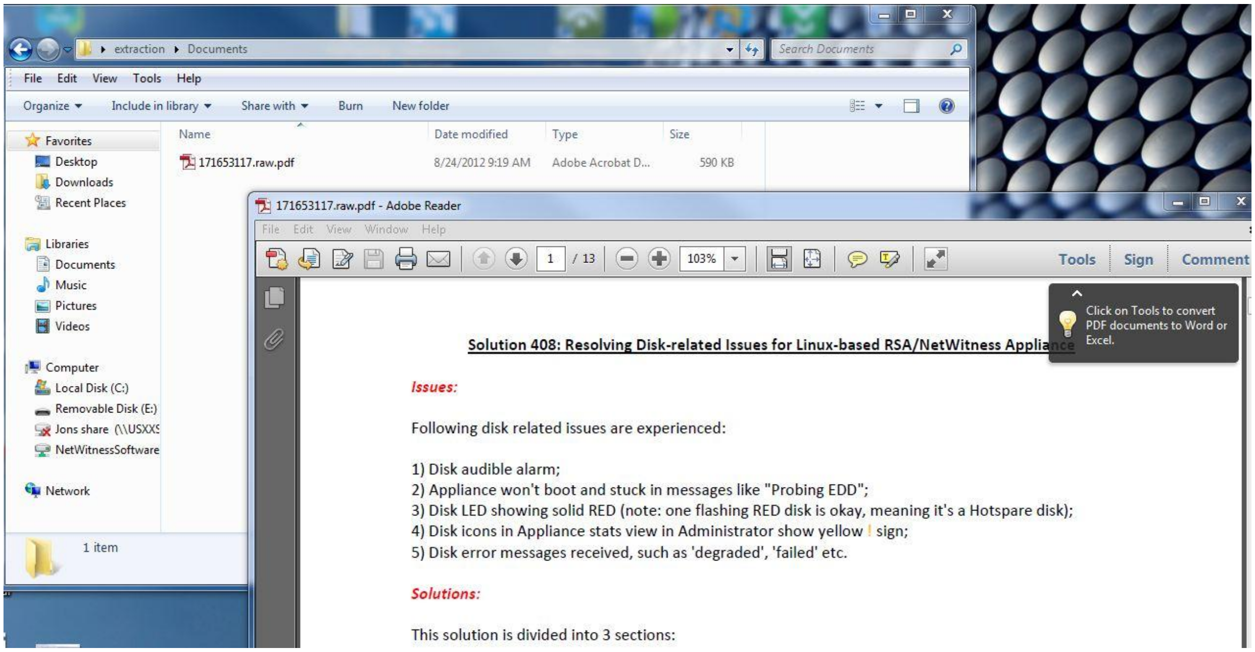
Directory: C:\Users[redacted]esktop\extraction

Subdirectory Organization By File Type

Enabled	Category	File Extensions
☑	Audio	.wav;.mp3;.aac;.au;.aiff;.jfif;.wma;.mpa;.ra;
☑	Video	.wmv;.flv;.mp4;.mpg;.swf;.avi;.mov;.asf;.vob;.rm;
☑	Documents	.doc;.wps;.pps;.ppt;.pptx;.xls;.xlsx;.wks;.pdf;.rtf;.odt;.ods;.odp;.odg;.odf;
☑	Web	.asp;.cer;.csr;.css;.htm;.html;.js;.jsp;.php;.rss;.xhtml;.xml;
☑	Images	.png;.gif;.jpg;.jpeg;.bmp;.tif;.tiff;.psd;.psp;
☑	Archives	.zip;.zipx;.rar;.tar;.gz;.sit;.sitx;.z;.cab;.7z;.iso;
☑	Executables	.exe;.rpm;.dmg;.bin;.app;.pkg;.dll;
☑	BitTorrent	.torrent;
☑	Other	*

-1.5
United States
thborough
2.2966
-71.5352
Corporation
Campus: Mike.Daly.flagler.edu
rid-s3-sm-62
29

In this example we chose to save the file in Desktop/extraction folder and it created a Documents folder and named the file **<SessionID>.raw.pdf.** Note - It may cause confusion that the filename gets changed.



Name	Date modified	Type	Size
171653117.raw.pdf	8/24/2012 9:19 AM	Adobe Acrobat D...	590 KB

Solution 408: Resolving Disk-related Issues for Linux-based RSA/NetWitness Appliance

Issues:

Following disk related issues are experienced:

1) Disk audible alarm;
2) Appliance won't boot and stuck in messages like "Probing EDD";
3) Disk LED showing solid RED (note: one flashing RED disk is okay, meaning it's a Hotspare disk);
4) Disk icons in Appliance stats view in Administrator show yellow ! sign;
5) Disk error messages received, such as 'degraded', 'failed' etc.

Solutions:

This solution is divided into 3 sections: