Fighting Cybercrime using Digital Forensics

UNIVERSITY OF PLYMOUTH

Session Outline

- Digital Forensics:
  - What is digital forensics
  - Forensic processes
  - Investigative mindset
  - Analysis of a suspect disk image
- Tools for this session:
  - Autopsy for Windows
  - Hunter XP demo case

What is Cybercrime?

The UK Government defines Cybercrime as:

- **Cyber-dependent crimes** - crimes that can be committed only through the use of Information and Communications Technology (‘ICT’) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
- **Cyber-enabled crimes** - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Source: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

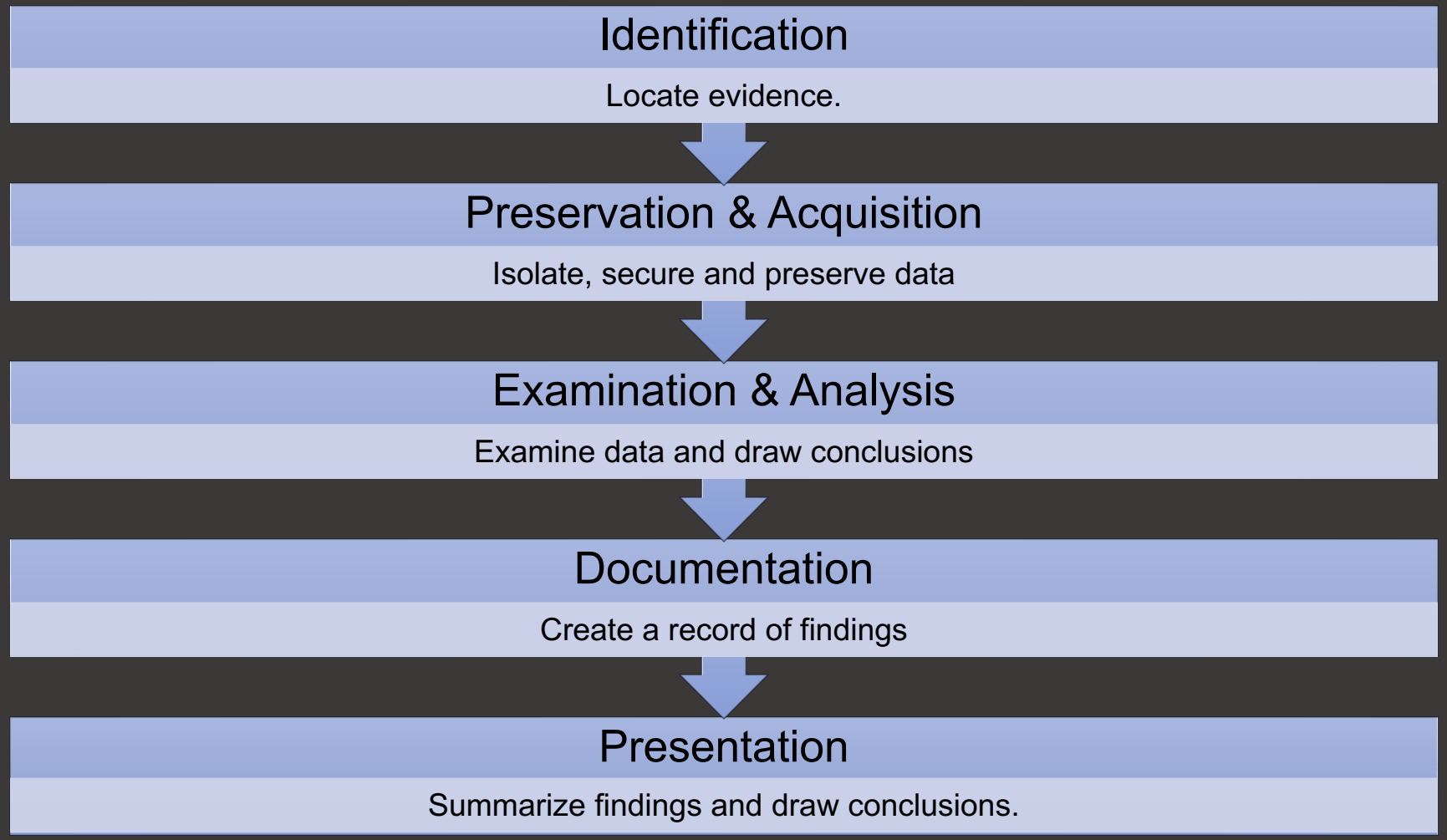
How do we deal with Cybercrime?

Digital Forensic Investigation

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Source: Digital Forensic Research Workshop (DFRWS), 2001

Forensic Process



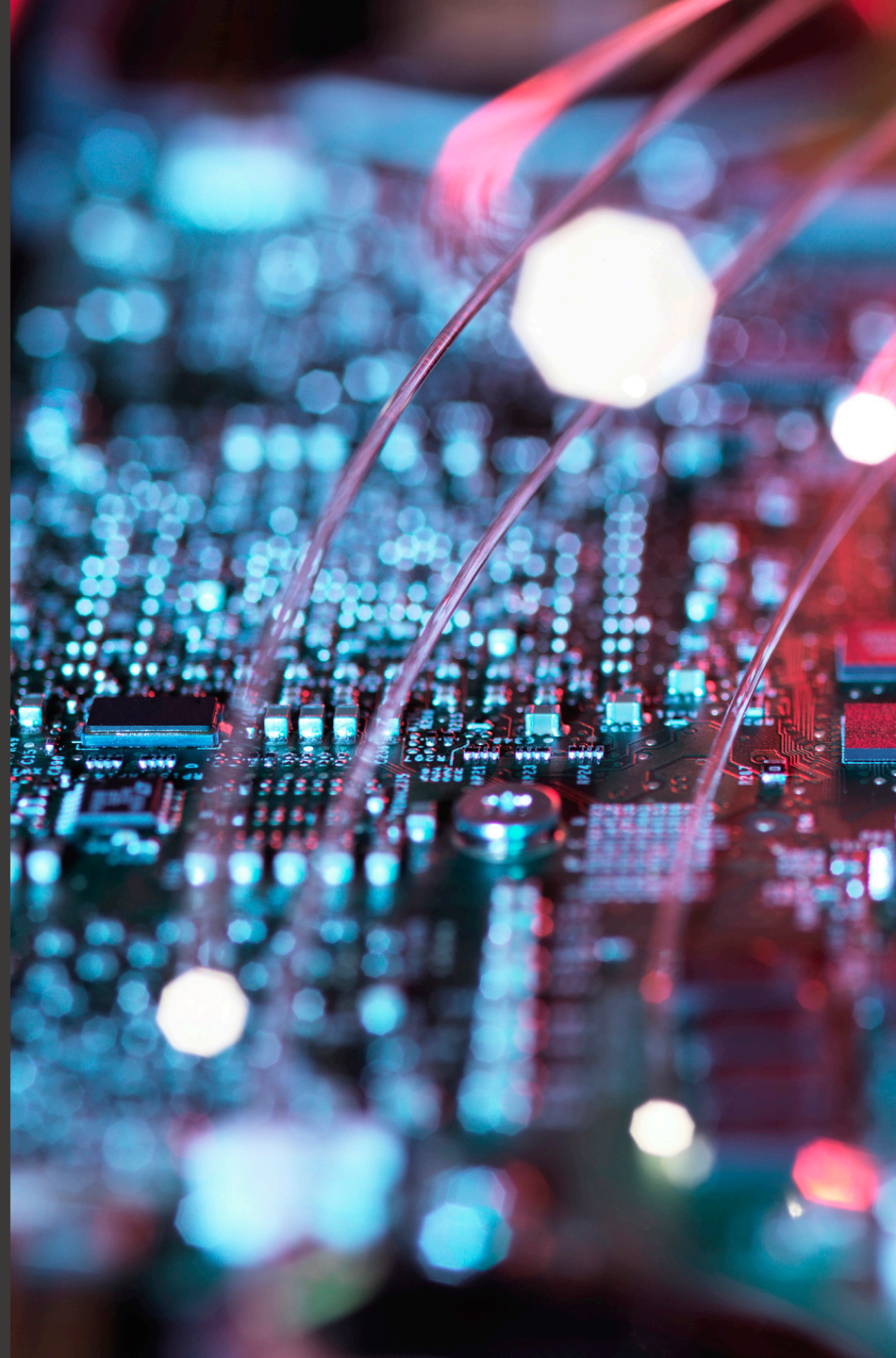
Acquisition

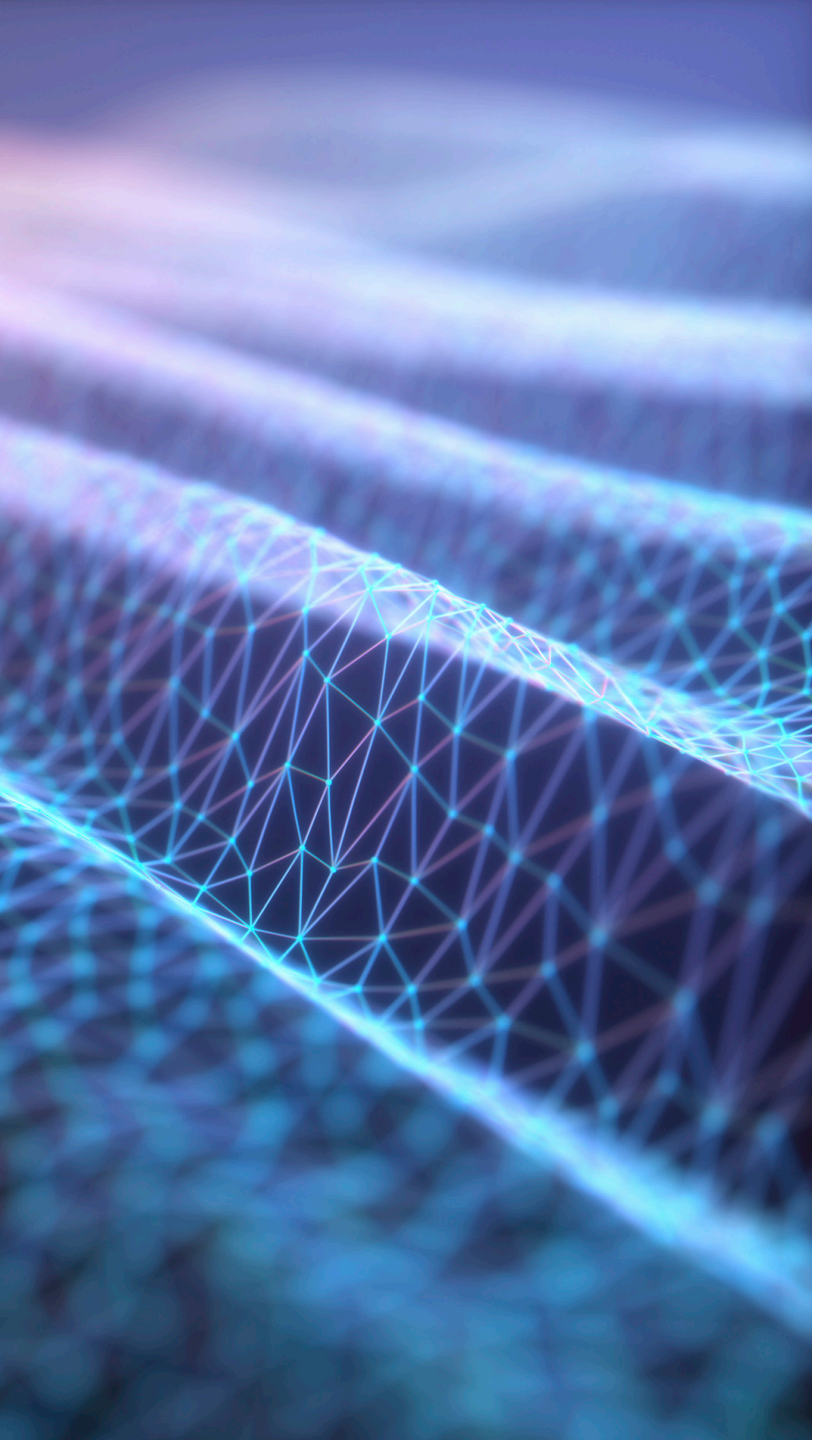
- Preservation of data is essential
  - Cloning suspect hard drive to an image file
- Hardware write blocker
  - Ensure that no new data is written to a suspect drive
- Documentation and chain of custody
  - Written records of each process followed and who carried out tasks involved.

Forensic Analysis

- **Dead analysis**
  - Examination of the suspect machine in a non-booted fashion.
  - Use of case management software.
  - Conducting operations on the suspect image or drive without modification.
- **Live analysis**
  - Examination of the suspects machine in a booted fashion.
  - Useful for understanding how a piece of malware is behaving.

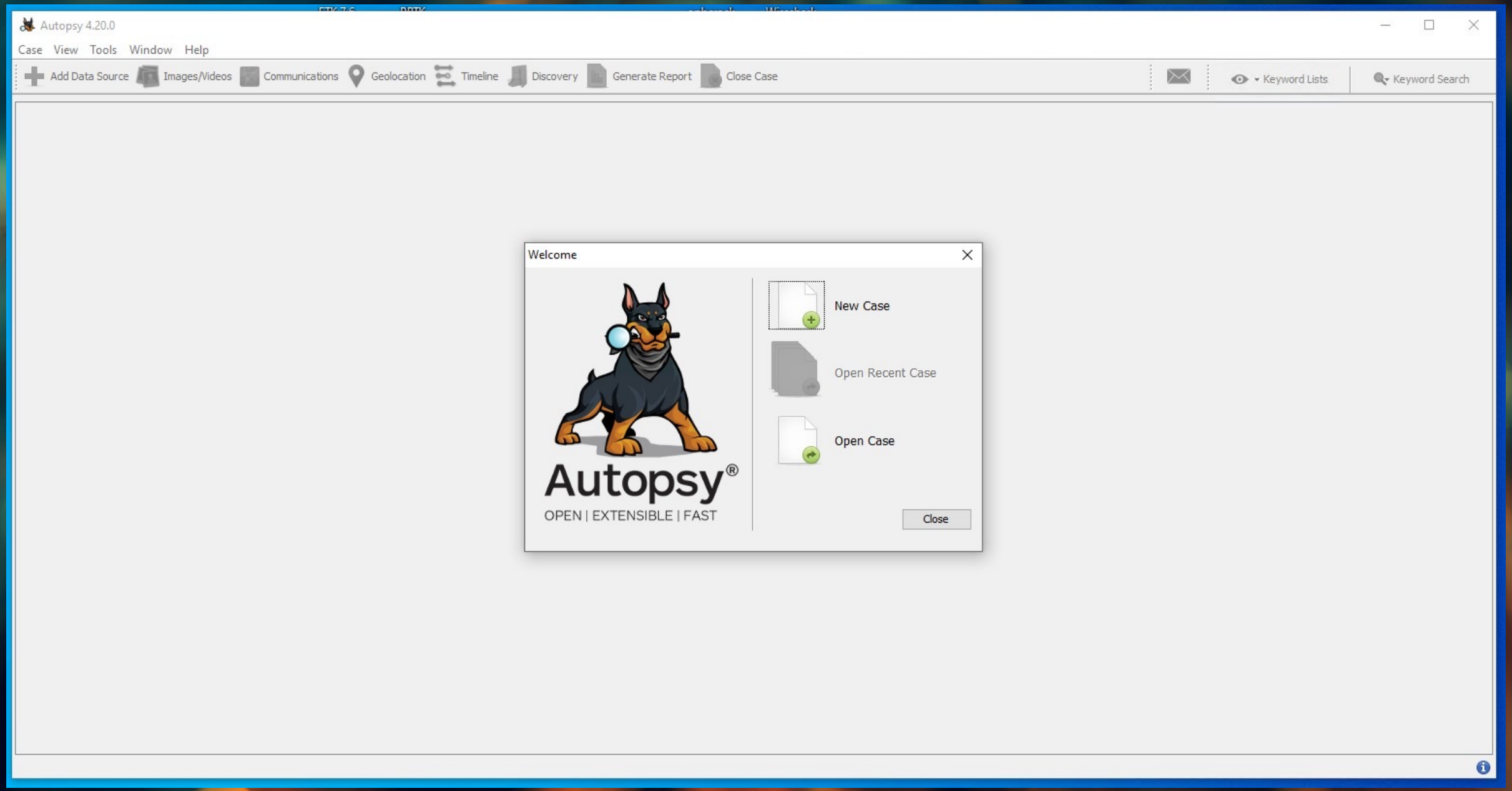
Examination & Analysis

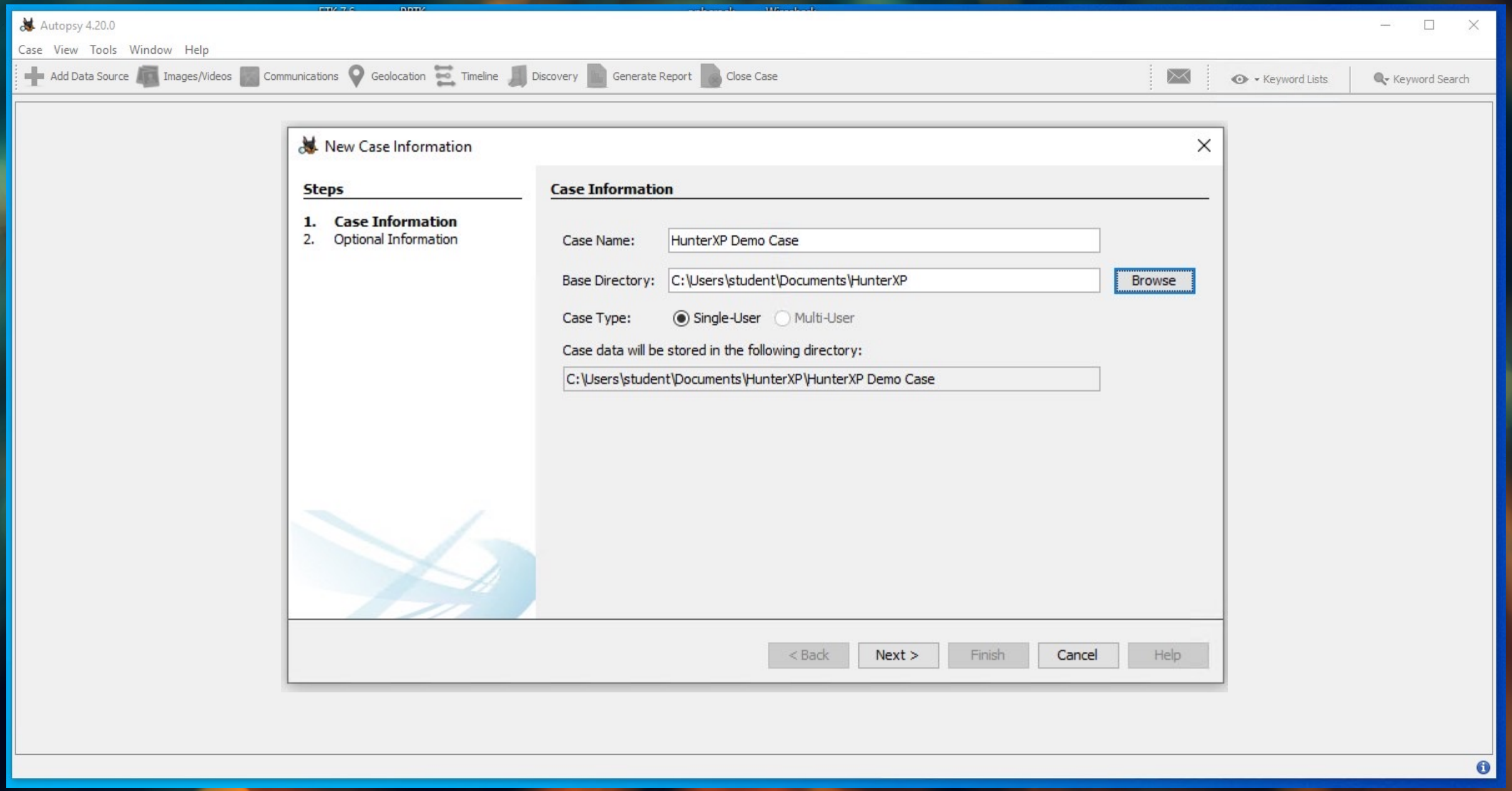


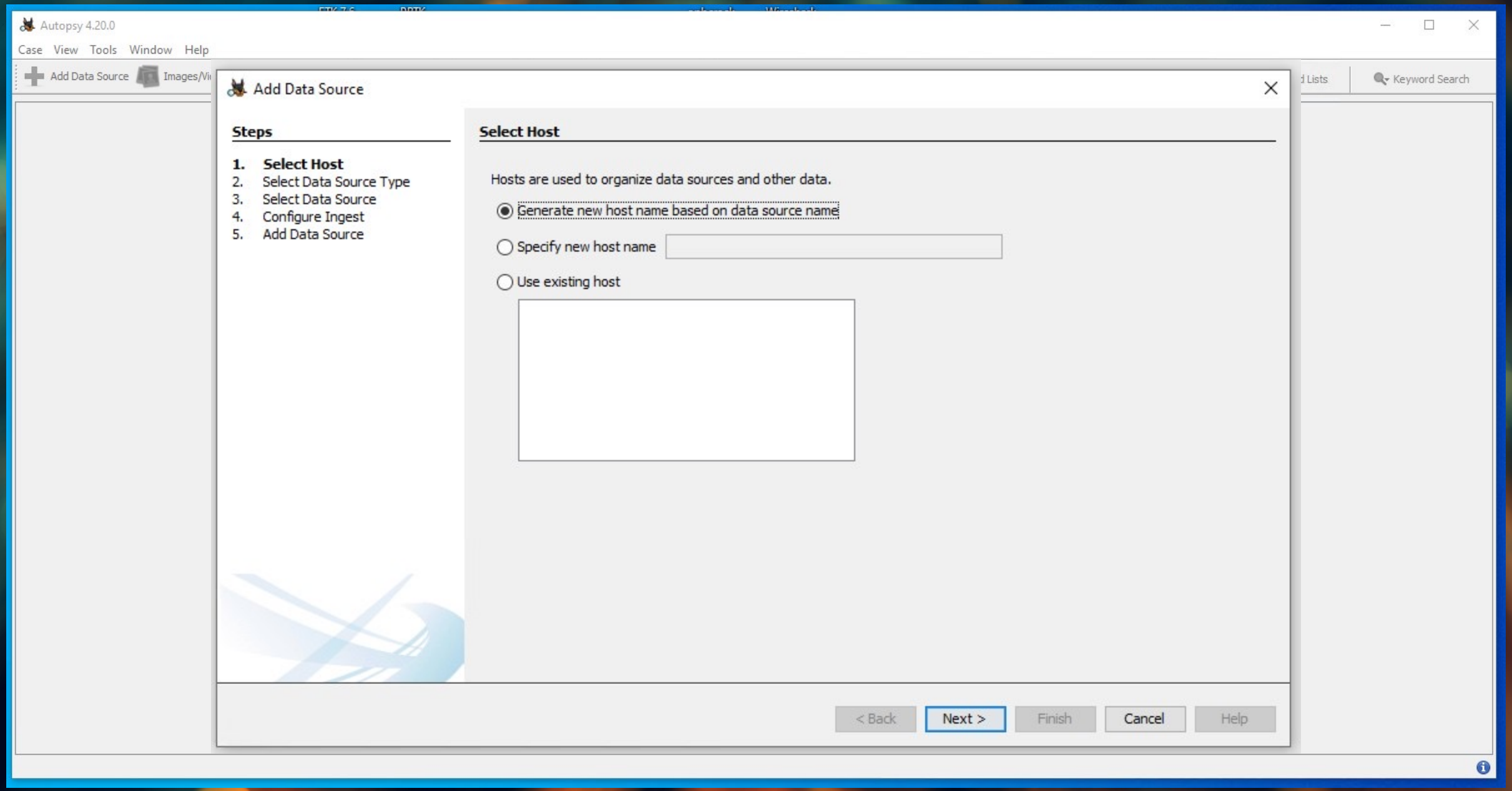


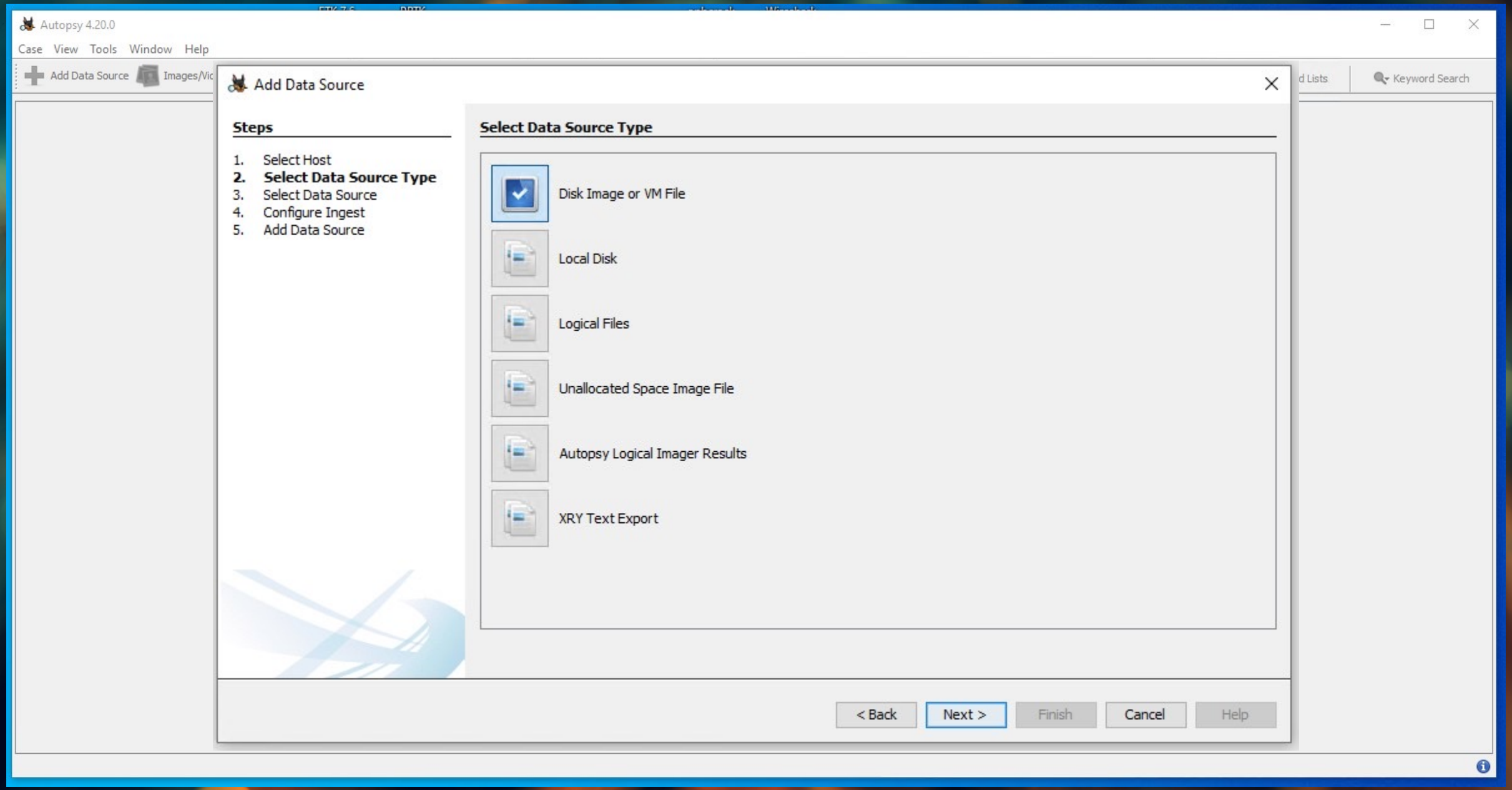
Activity: Autopsy

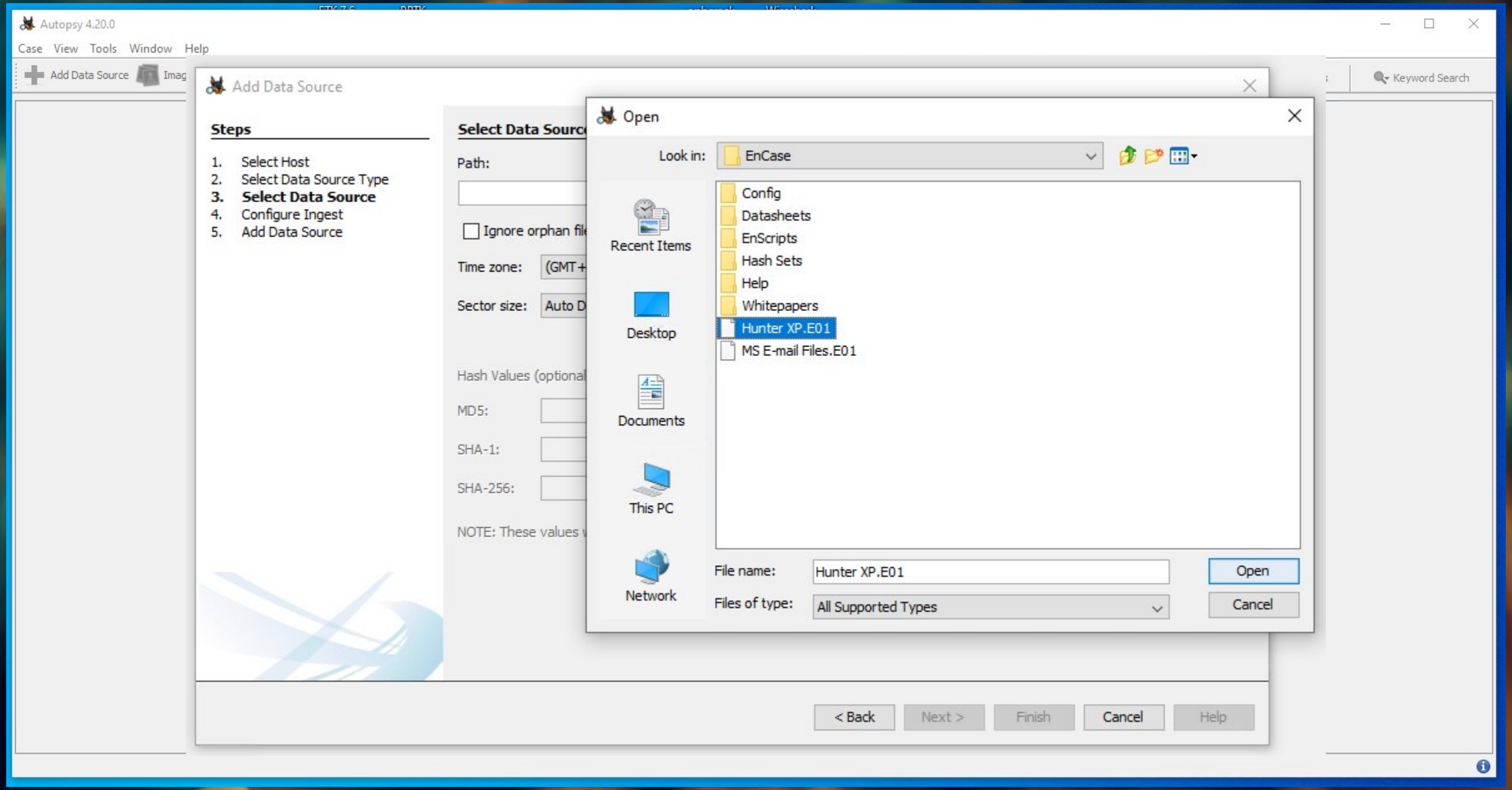
1. Open Autopsy 4.20.0
2. Add a new case.
3. Enter a name for your case and select a base directory, such as in your documents area.
4. Select Host: Generate new host name based on data source.
5. Import the ‘Hunter XP’ disk image.
6. Leave the ingestion options as they are and click next.
7. Click finish once the ingestion has completed.

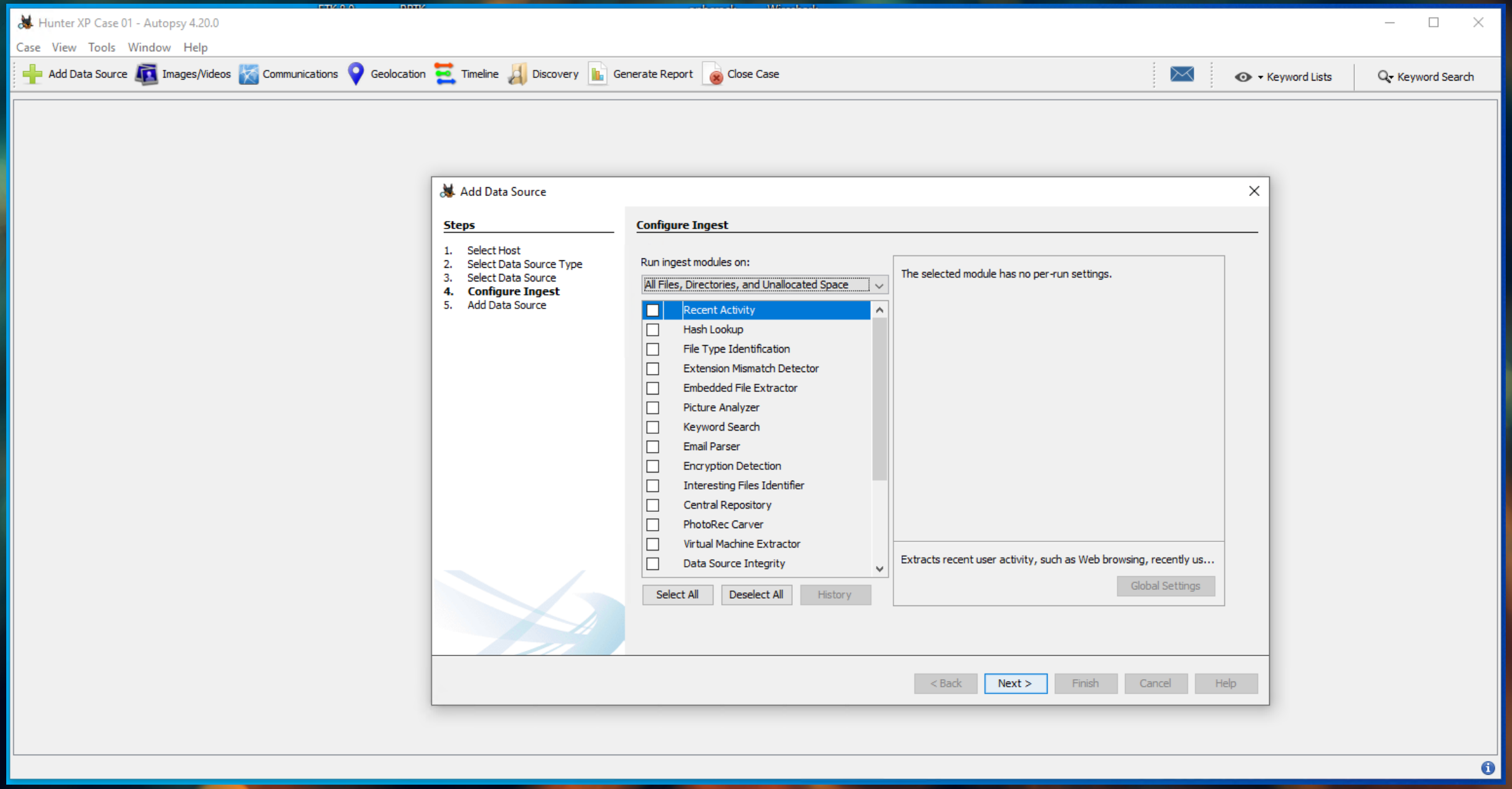

Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Close
Autopsy®
OPEN | EXTENSIBLE | FAST

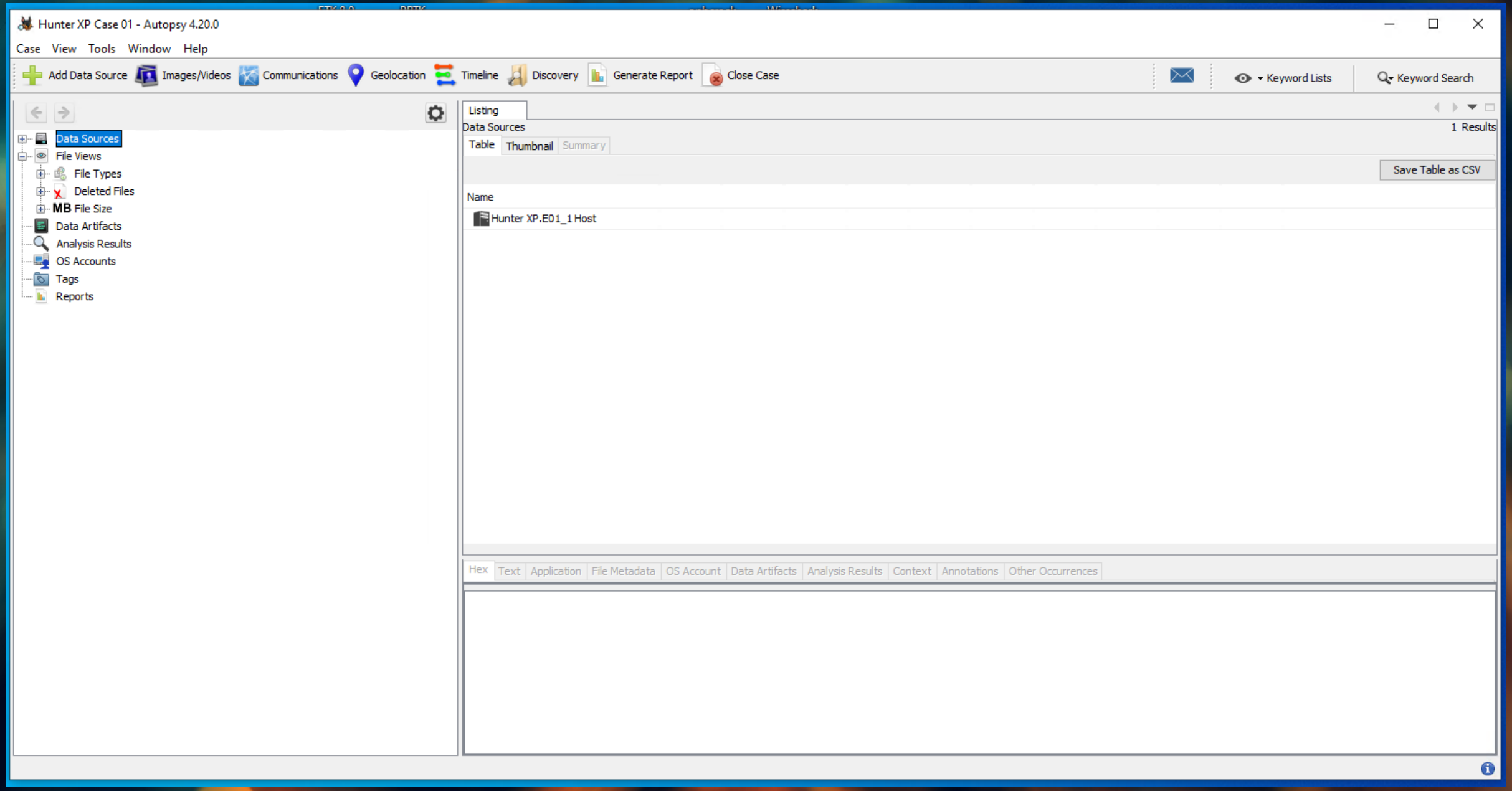

Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
HunterXP Demo Case
Base Directory:
C:\Users\student\Documents\HunterXP
Browse
Case Type:
Single-User
Multi-User
Case data will be stored in the following directory:
C:\Users\student\Documents\HunterXP\HunterXP Demo Case
< Back
Next >
Finish
Cancel
Help

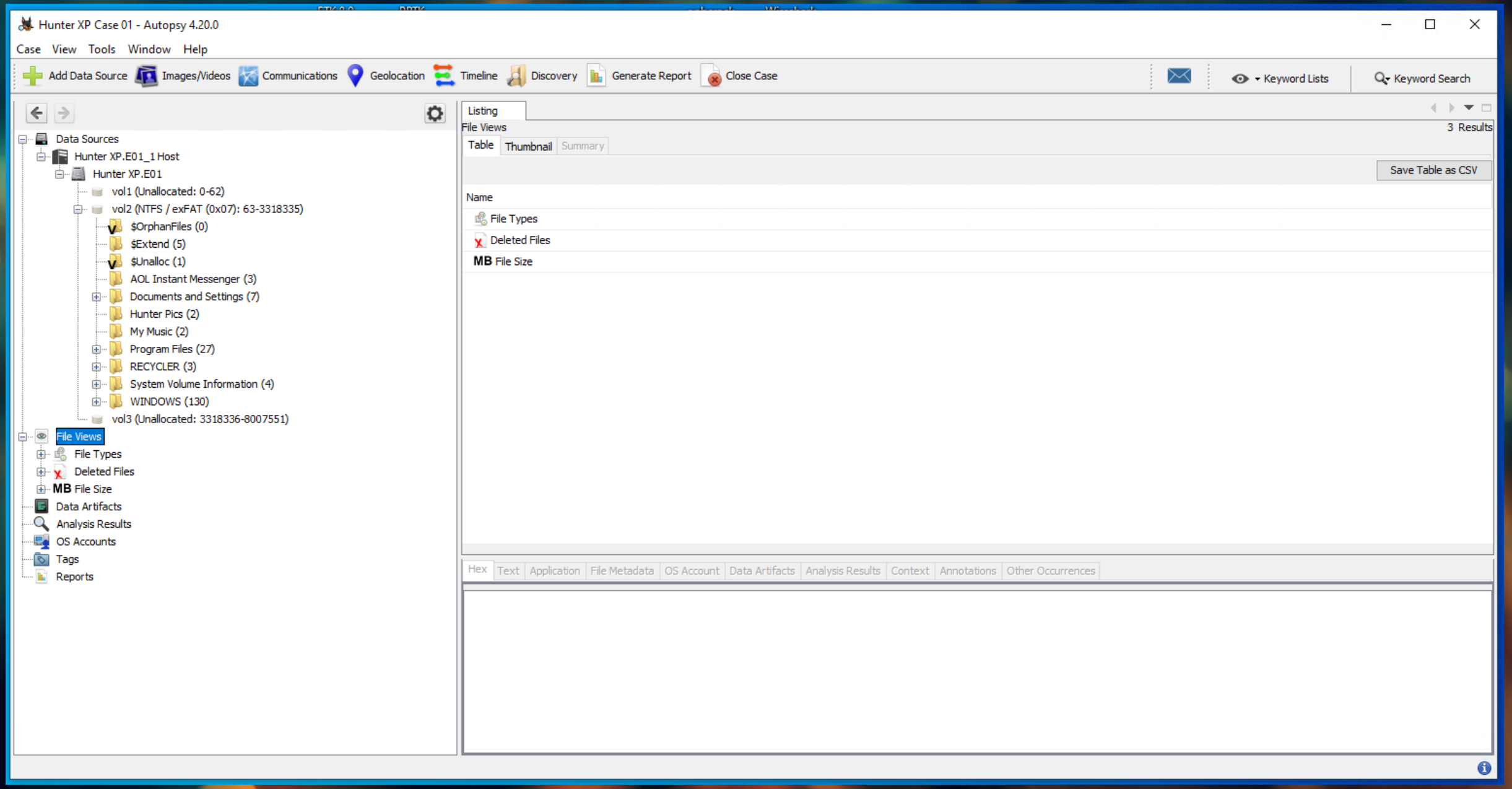

Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Vi
Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

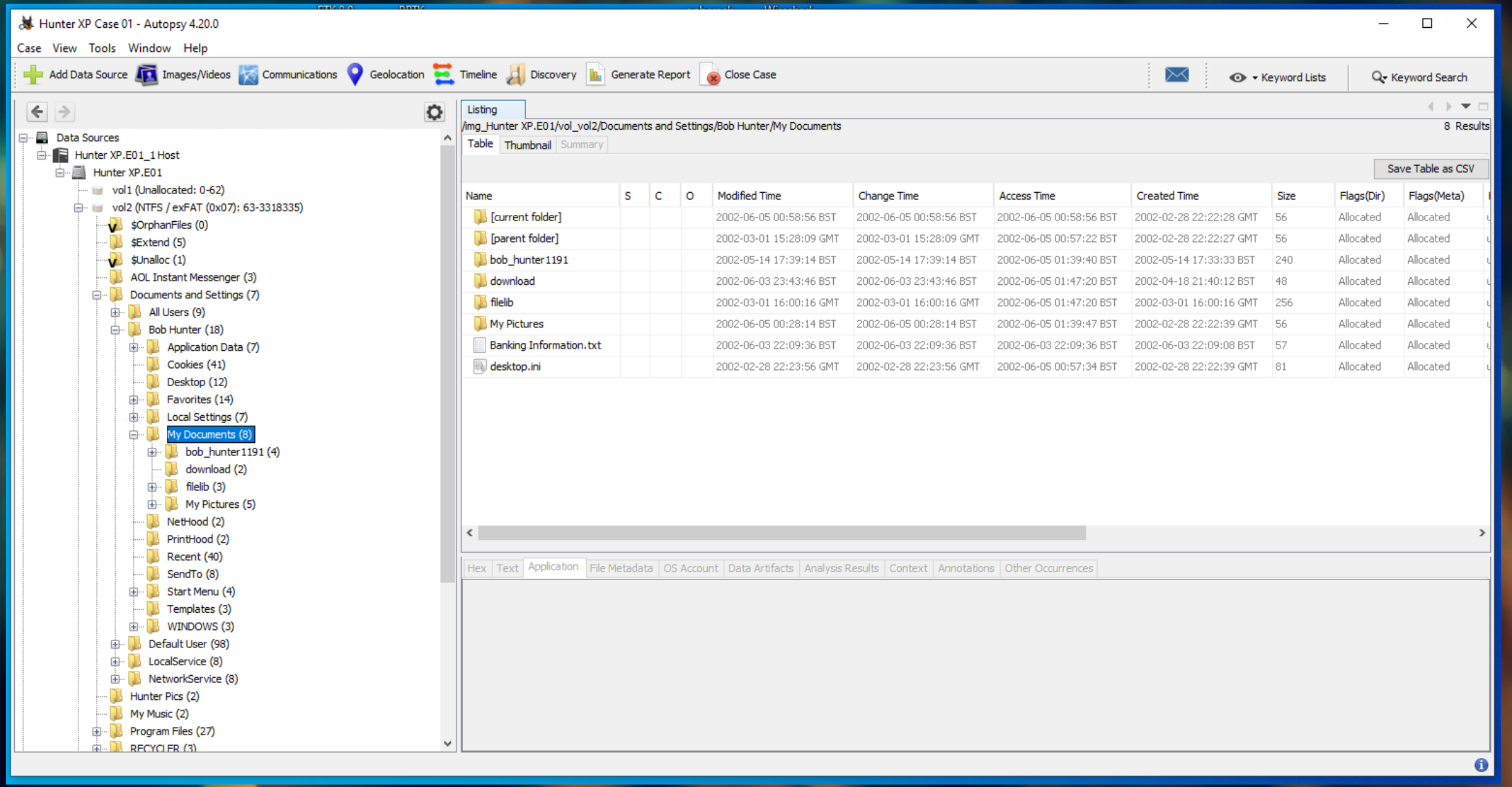

Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Vic
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

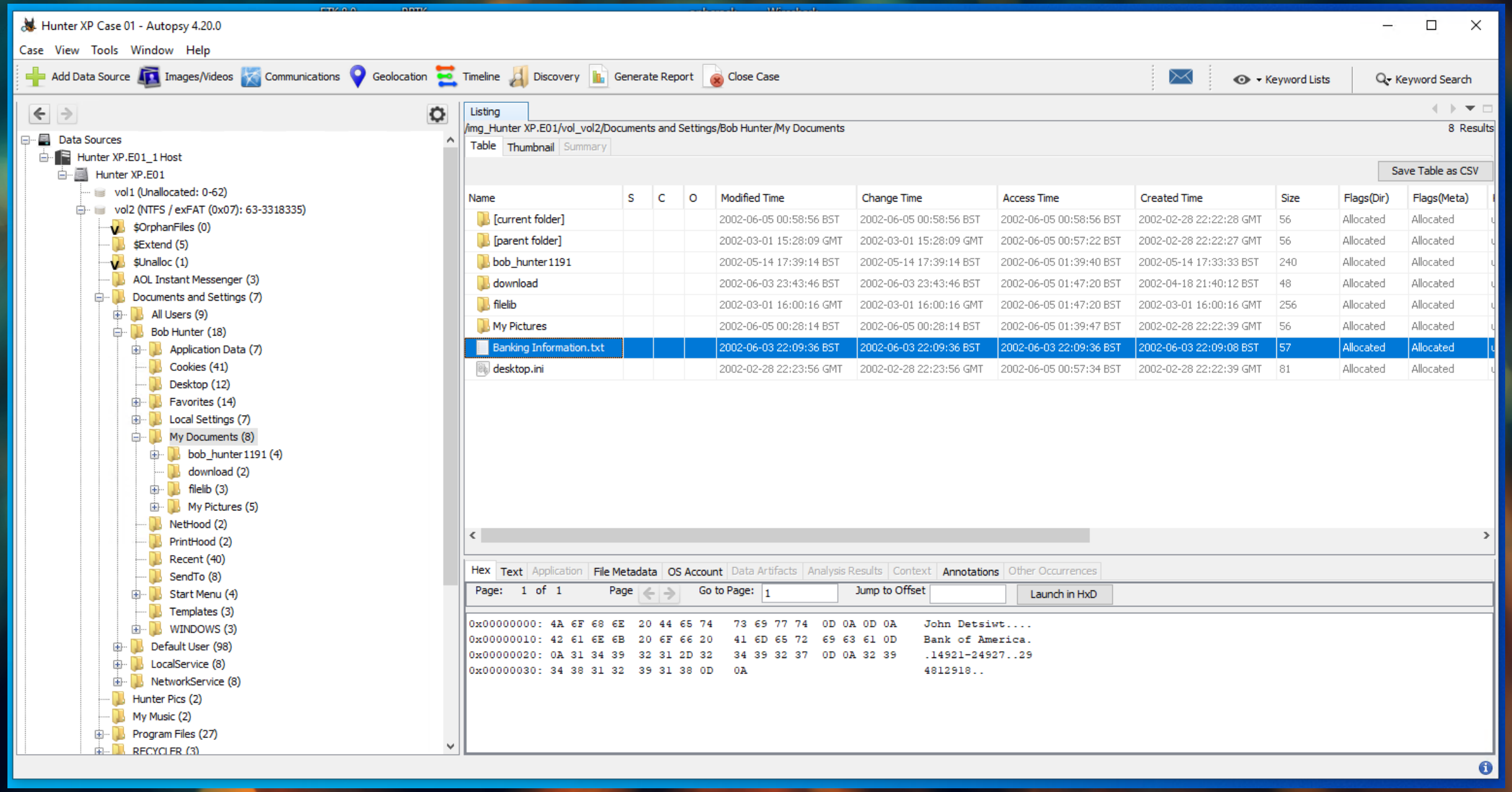

Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
Ignore orphan files
Time zone:
Sector size:
Hash Values (optional)
MD5:
SHA-1:
SHA-256:
NOTE: These values
< Back
Next >
Finish
Cancel
Help
Open
Look in:
EnCase
Recent Items
Desktop
Documents
This PC
Network
Config
Datasheets
EnScripts
Hash Sets
Help
Whitepapers
Hunter XP.E01
MS E-mail Files.E01
File name:
Hunter XP.E01
Files of type:
All Supported Types
Open
Cancel

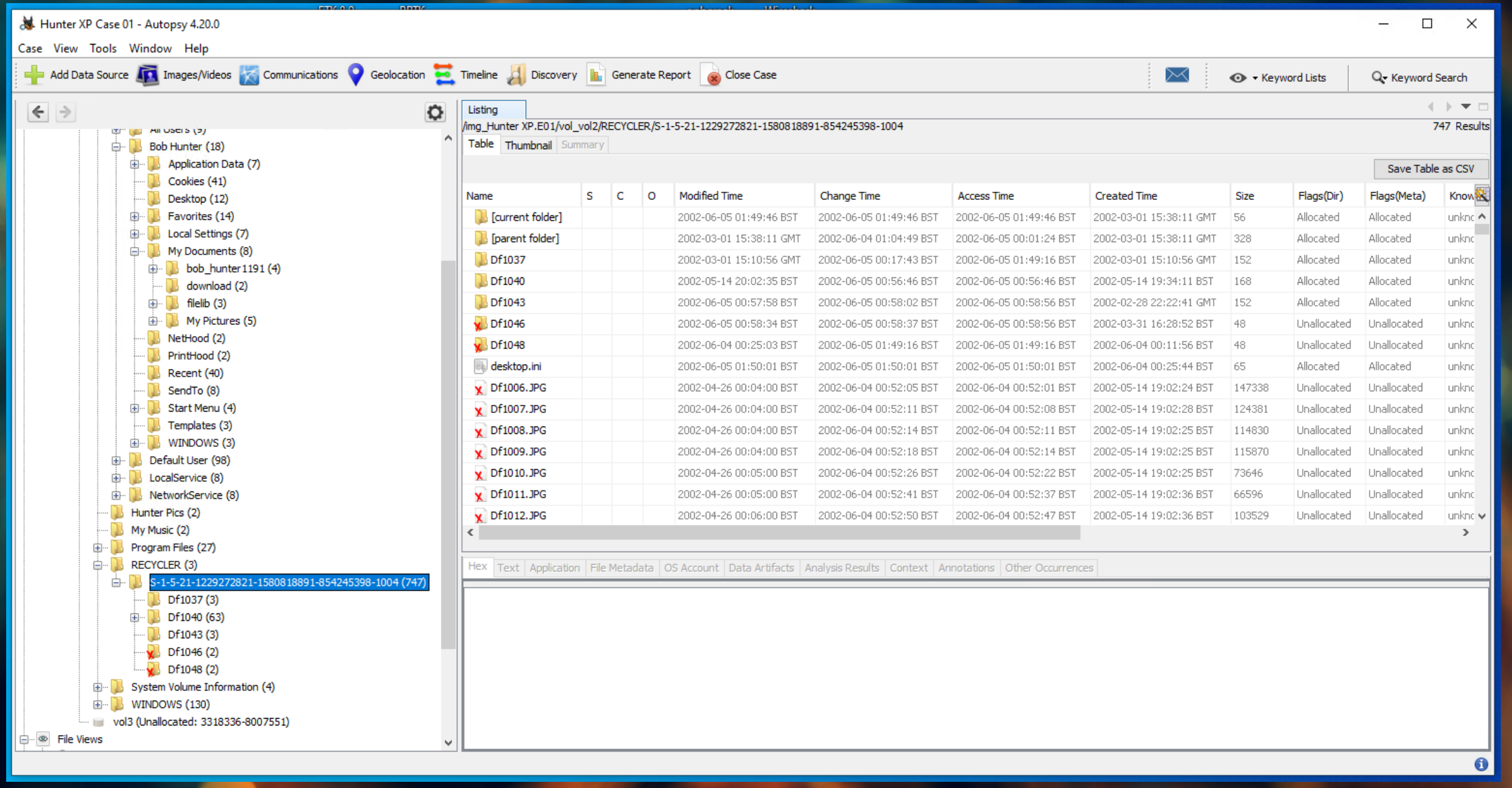

Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help

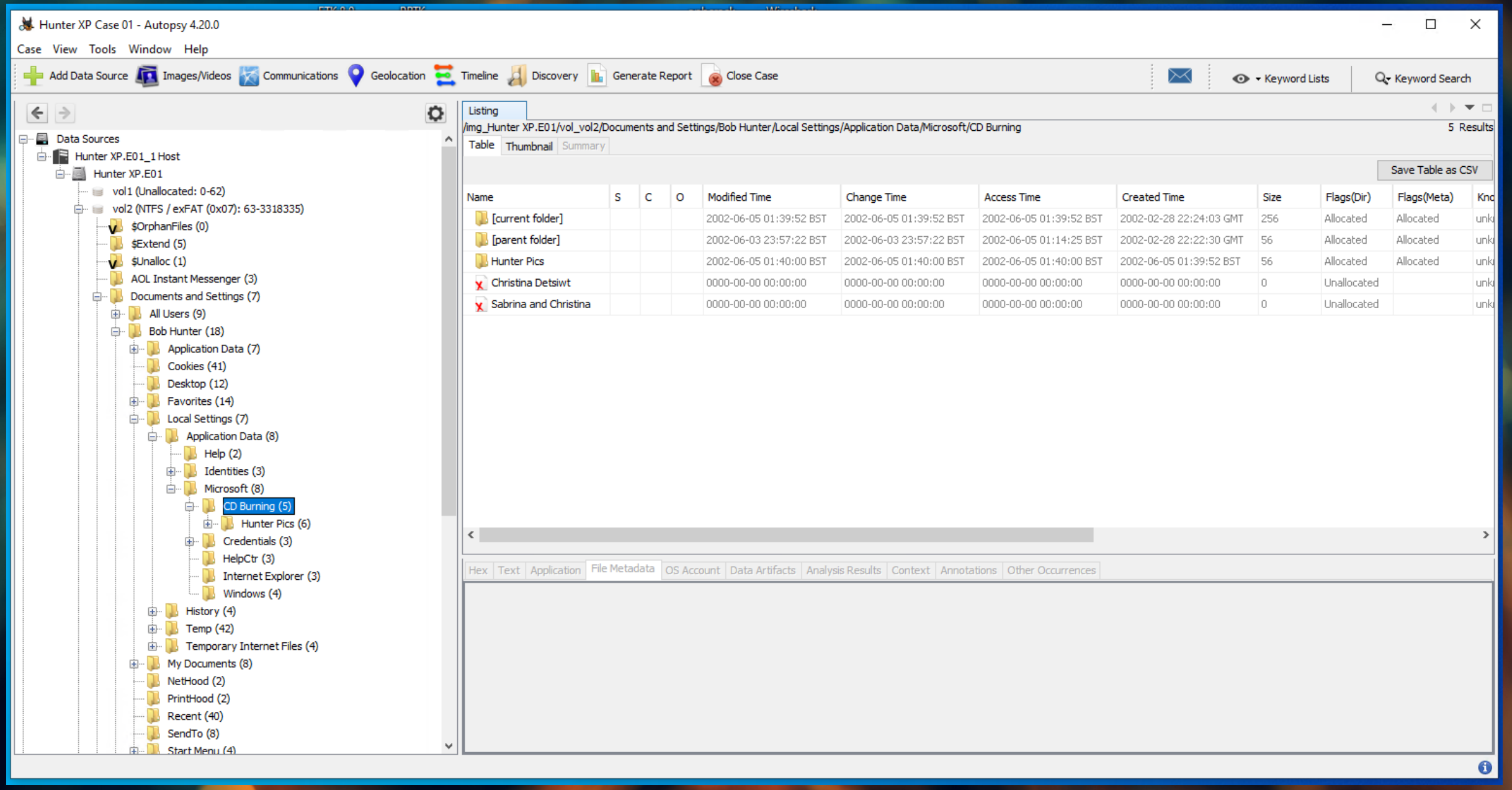

Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Reports
Listing
Data Sources
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
Hunter XP.E01_1 Host
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Hunter XP.E01_1 Host
Hunter XP.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
Hunter Pics (2)
My Music (2)
Program Files (27)
RECYCLER (3)
System Volume Information (4)
WINDOWS (130)
vol3 (Unallocated: 3318336-8007551)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Reports
Listing
File Views
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
File Types
Deleted Files
MB File Size
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Hunter XP.E01_1 Host
Hunter XP.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
All Users (9)
Bob Hunter (18)
Application Data (7)
Cookies (41)
Desktop (12)
Favorites (14)
Local Settings (7)
My Documents (8)
bob_hunter1191 (4)
download (2)
filelib (3)
My Pictures (5)
NetHood (2)
PrintHood (2)
Recent (40)
SendTo (8)
Start Menu (4)
Templates (3)
WINDOWS (3)
Default User (98)
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
RECYCLER (3)
Listing
/img_Hunter XP.E01/vol_vol2/Documents and Settings/Bob Hunter/My Documents
8 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta)
[current folder] 2002-06-05 00:58:56 BST 2002-06-05 00:58:56 BST 2002-06-05 00:58:56 BST 2002-02-28 22:22:28 GMT 56 Allocated Allocated
[parent folder] 2002-03-01 15:28:09 GMT 2002-03-01 15:28:09 GMT 2002-06-05 00:57:22 BST 2002-02-28 22:22:27 GMT 56 Allocated Allocated
bob_hunter1191 2002-05-14 17:39:14 BST 2002-05-14 17:39:14 BST 2002-06-05 01:39:40 BST 2002-05-14 17:33:33 BST 240 Allocated Allocated
download 2002-06-03 23:43:46 BST 2002-06-03 23:43:46 BST 2002-06-05 01:47:20 BST 2002-04-18 21:40:12 BST 48 Allocated Allocated
filelib 2002-03-01 16:00:16 GMT 2002-03-01 16:00:16 GMT 2002-06-05 01:47:20 BST 2002-03-01 16:00:16 GMT 256 Allocated Allocated
My Pictures 2002-06-05 00:28:14 BST 2002-06-05 00:28:14 BST 2002-06-05 01:39:47 BST 2002-02-28 22:22:39 GMT 56 Allocated Allocated
Banking Information.txt 2002-06-03 22:09:36 BST 2002-06-03 22:09:36 BST 2002-06-03 22:09:36 BST 2002-06-03 22:09:08 BST 57 Allocated Allocated
desktop.ini 2002-02-28 22:23:56 GMT 2002-02-28 22:23:56 GMT 2002-06-05 00:57:34 BST 2002-02-28 22:22:39 GMT 81 Allocated Allocated
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Hunter XP.E01_1 Host
Hunter XP.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
All Users (9)
Bob Hunter (18)
Application Data (7)
Cookies (41)
Desktop (12)
Favorites (14)
Local Settings (7)
My Documents (8)
bob_hunter1191 (4)
download (2)
filelib (3)
My Pictures (5)
NetHood (2)
PrintHood (2)
Recent (40)
SendTo (8)
Start Menu (4)
Templates (3)
WINDOWS (3)
Default User (98)
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
RECYCLER (3)
Listing
/img_Hunter XP.E01/vol_vol2/Documents and Settings/Bob Hunter/My Documents
8 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta)
[current folder] 2002-06-05 00:58:56 BST 2002-06-05 00:58:56 BST 2002-06-05 00:58:56 BST 2002-02-28 22:22:28 GMT 56 Allocated Allocated
[parent folder] 2002-03-01 15:28:09 GMT 2002-03-01 15:28:09 GMT 2002-06-05 00:57:22 BST 2002-02-28 22:22:27 GMT 56 Allocated Allocated
bob_hunter1191 2002-05-14 17:39:14 BST 2002-05-14 17:39:14 BST 2002-06-05 01:39:40 BST 2002-05-14 17:33:33 BST 240 Allocated Allocated
download 2002-06-03 23:43:46 BST 2002-06-03 23:43:46 BST 2002-06-05 01:47:20 BST 2002-04-18 21:40:12 BST 48 Allocated Allocated
filelib 2002-03-01 16:00:16 GMT 2002-03-01 16:00:16 GMT 2002-06-05 01:47:20 BST 2002-03-01 16:00:16 GMT 256 Allocated Allocated
My Pictures 2002-06-05 00:28:14 BST 2002-06-05 00:28:14 BST 2002-06-05 01:39:47 BST 2002-02-28 22:22:39 GMT 56 Allocated Allocated
Banking Information.txt 2002-06-03 22:09:36 BST 2002-06-03 22:09:36 BST 2002-06-03 22:09:36 BST 2002-06-03 22:09:08 BST 57 Allocated Allocated
desktop.ini 2002-02-28 22:23:56 GMT 2002-02-28 22:23:56 GMT 2002-06-05 00:57:34 BST 2002-02-28 22:22:39 GMT 81 Allocated Allocated
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 1 Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000000: 4A 6F 68 6E 20 44 65 74 73 69 77 74 0D 0A 0D 0A John Detsiwt....
0x00000010: 42 61 6E 6B 20 6F 66 20 41 6D 65 72 69 63 61 0D Bank of America.
0x00000020: 0A 31 34 39 32 31 2D 32 34 39 32 37 0D 0A 32 39 .14921-24927..29
0x00000030: 34 38 31 32 39 31 38 0D 0A 4812918..


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Bob Hunter (18)
Application Data (7)
Cookies (41)
Desktop (12)
Favorites (14)
Local Settings (7)
My Documents (8)
bob_hunter1191 (4)
download (2)
filelib (3)
My Pictures (5)
NetHood (2)
PrintHood (2)
Recent (40)
SendTo (8)
Start Menu (4)
Templates (3)
WINDOWS (3)
Default User (98)
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
RECYCLER (3)
S-1-5-21-1229272821-1580818891-854245398-1004 (747)
Df1037 (3)
Df1040 (63)
Df1043 (3)
Df1046 (2)
Df1048 (2)
System Volume Information (4)
WINDOWS (130)
vol3 (Unallocated: 3318336-8007551)
File Views
Listing
/img_Hunter XP.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004
747 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known
[current folder] 2002-06-05 01:49:46 BST 2002-06-05 01:49:46 BST 2002-06-05 01:49:46 BST 2002-03-01 15:38:11 GMT 56 Allocated Allocated unknc
[parent folder] 2002-03-01 15:38:11 GMT 2002-06-04 01:04:49 BST 2002-06-05 00:01:24 BST 2002-03-01 15:38:11 GMT 328 Allocated Allocated unknc
Df1037 2002-03-01 15:10:56 GMT 2002-06-05 00:17:43 BST 2002-06-05 01:49:16 BST 2002-03-01 15:10:56 GMT 152 Allocated Allocated unknc
Df1040 2002-05-14 20:02:35 BST 2002-06-05 00:56:46 BST 2002-06-05 00:56:46 BST 2002-05-14 19:34:11 BST 168 Allocated Allocated unknc
Df1043 2002-06-05 00:57:58 BST 2002-06-05 00:58:02 BST 2002-06-05 00:58:56 BST 2002-02-28 22:22:41 GMT 152 Allocated Allocated unknc
Df1046 2002-06-05 00:58:34 BST 2002-06-05 00:58:37 BST 2002-06-05 00:58:56 BST 2002-03-31 16:28:52 BST 48 Unallocated Unallocated unknc
Df1048 2002-06-04 00:25:03 BST 2002-06-05 01:49:16 BST 2002-06-05 01:49:16 BST 2002-06-04 00:11:56 BST 48 Unallocated Unallocated unknc
desktop.ini 2002-06-05 01:50:01 BST 2002-06-05 01:50:01 BST 2002-06-05 01:50:01 BST 2002-06-04 00:25:44 BST 65 Allocated Allocated unknc
Df1006.JPG 2002-04-26 00:04:00 BST 2002-06-04 00:52:05 BST 2002-06-04 00:52:01 BST 2002-05-14 19:02:24 BST 147338 Unallocated Unallocated unknc
Df1007.JPG 2002-04-26 00:04:00 BST 2002-06-04 00:52:11 BST 2002-06-04 00:52:08 BST 2002-05-14 19:02:28 BST 124381 Unallocated Unallocated unknc
Df1008.JPG 2002-04-26 00:04:00 BST 2002-06-04 00:52:14 BST 2002-06-04 00:52:11 BST 2002-05-14 19:02:25 BST 114830 Unallocated Unallocated unknc
Df1009.JPG 2002-04-26 00:04:00 BST 2002-06-04 00:52:18 BST 2002-06-04 00:52:14 BST 2002-05-14 19:02:25 BST 115870 Unallocated Unallocated unknc
Df1010.JPG 2002-04-26 00:05:00 BST 2002-06-04 00:52:26 BST 2002-06-04 00:52:22 BST 2002-05-14 19:02:25 BST 73646 Unallocated Unallocated unknc
Df1011.JPG 2002-04-26 00:05:00 BST 2002-06-04 00:52:41 BST 2002-06-04 00:52:37 BST 2002-05-14 19:02:36 BST 66596 Unallocated Unallocated unknc
Df1012.JPG 2002-04-26 00:06:00 BST 2002-06-04 00:52:50 BST 2002-06-04 00:52:47 BST 2002-05-14 19:02:36 BST 103529 Unallocated Unallocated unknc
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Hunter XP.E01_1 Host
Hunter XP.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
All Users (9)
Bob Hunter (18)
Application Data (7)
Cookies (41)
Desktop (12)
Favorites (14)
Local Settings (7)
Application Data (8)
Help (2)
Identities (3)
Microsoft (8)
CD Burning (5)
Hunter Pics (6)
Credentials (3)
HelpCtr (3)
Internet Explorer (3)
Windows (4)
History (4)
Temp (42)
Temporary Internet Files (4)
My Documents (8)
NetHood (2)
PrintHood (2)
Recent (40)
SendTo (8)
Start Menu (4)
Listing
/img_Hunter XP.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning
5 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Kno
[current folder] 2002-06-05 01:39:52 BST 2002-06-05 01:39:52 BST 2002-06-05 01:39:52 BST 2002-02-28 22:24:03 GMT 256 Allocated Allocated unk
[parent folder] 2002-06-03 23:57:22 BST 2002-06-03 23:57:22 BST 2002-06-05 01:14:25 BST 2002-02-28 22:22:30 GMT 56 Allocated Allocated unk
Hunter Pics 2002-06-05 01:40:00 BST 2002-06-05 01:40:00 BST 2002-06-05 01:40:00 BST 2002-06-05 01:39:52 BST 56 Allocated Allocated unk
Christina Detsiwt 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated unk
Sabrina and Christina 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated unk
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Hunter XP Case 01 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

- 1041 (2)
- 1042 (2)
- 1054 (2)
- 2052 (2)
- 3076 (2)
- 3com_dmi (2)
- CatRoot (4)
- CatRoot2 (9)
- Com (9)
- config (23)
- dhcp (2)
- DirectX (3)
- dllcache (32)
- drivers (187)
- export (2)
- ias (4)
- icsxml (7)
- IME (5)
- inetsrv (2)
- Macromed (7)
- MsDtc (4)
- mui (4)
- npp (4)
- oobe (45)
- ras (8)
- Restore (6)
- Setup (17)
- ShellExt (2)
- spool (5)
  - drivers (4)
  - PRINTERS (45)
  - prtprocs (3)
- usmt (23)
- wbem (129)
- wins (2)
- xircom (2)

Listing

/img_Hunter XP.E01/vol_vol2/WINDOWS/system32/spool/PRINTERS 45 Results

Table | Thumbnail | Summary

Save Table as CSV

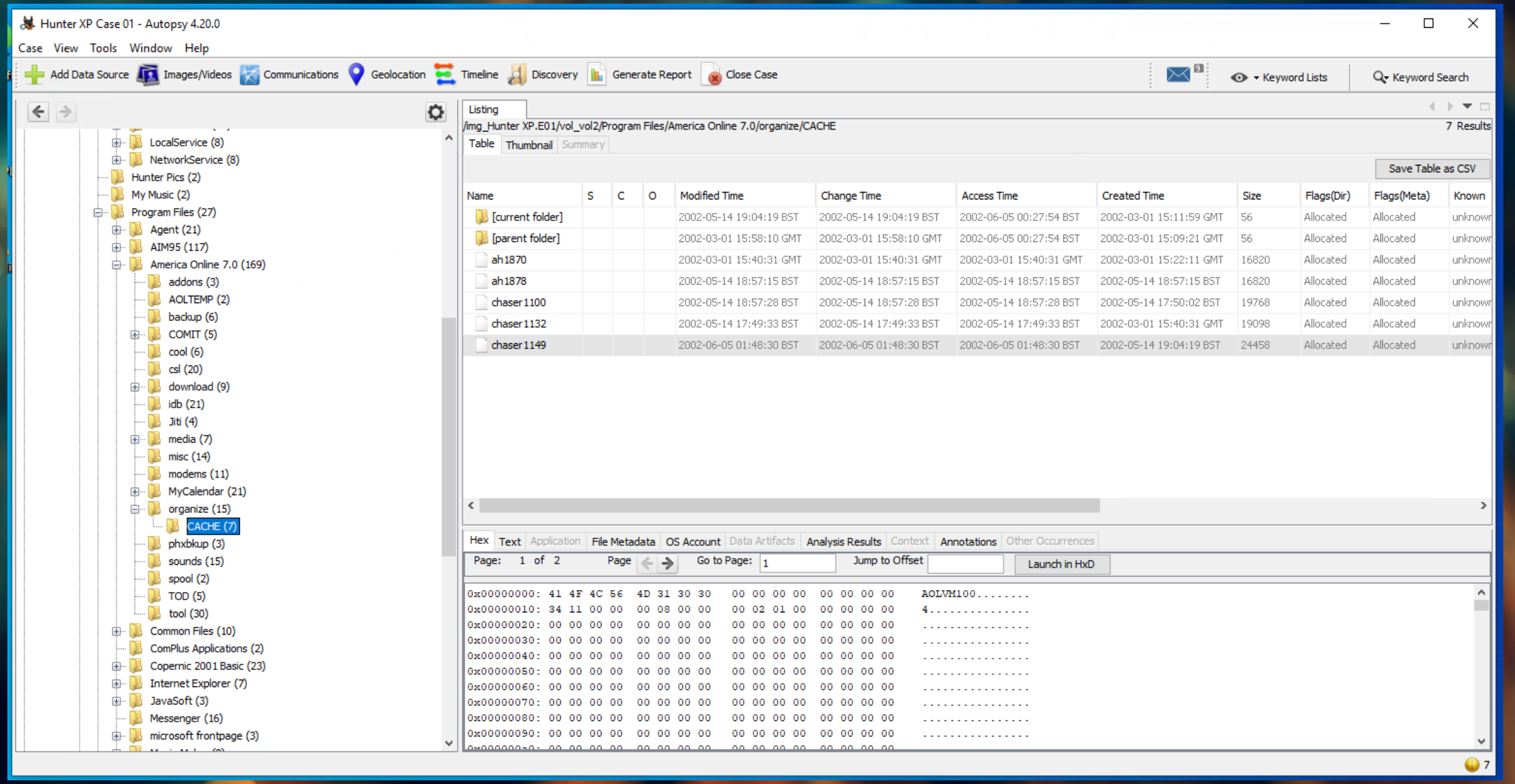
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
00017.SPL				2002-06-05 01:10:57 BST	2002-06-05 01:10:57 BST	2002-06-05 01:10:57 BST	2002-06-05 01:10:57 BST	345052	Allocated	Allocated	unkn
00018.SHD				2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	1360	Allocated	Allocated	unkn
00018.SPL				2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	2002-06-05 01:11:37 BST	941248	Allocated	Allocated	unkn
00019.SHD				2002-06-05 01:18:11 BST	2002-06-05 01:18:11 BST	2002-06-05 01:18:11 BST	2002-06-05 01:18:11 BST	1412	Allocated	Allocated	unkn
00019.SPL				2002-06-05 01:18:11 BST	2002-06-05 01:18:11 BST	2002-06-05 01:18:10 BST	2002-06-05 01:18:10 BST	394748	Allocated	Allocated	unkn
00020.SHD				2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	1372	Allocated	Allocated	unkn
00020.SPL				2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	2002-06-05 01:18:31 BST	524724	Allocated	Allocated	unkn
00021.SHD				2002-06-05 01:22:25 BST	2002-06-05 01:22:25 BST	2002-06-05 01:22:25 BST	2002-06-05 01:22:25 BST	1372	Allocated	Allocated	unkn
00021.SPL				2002-06-05 01:22:25 BST	2002-06-05 01:22:25 BST	2002-06-05 01:22:24 BST	2002-06-05 01:22:24 BST	1216240	Allocated	Allocated	unkn
00022.SHD				2002-06-05 01:41:04 BST	2002-06-05 01:41:04 BST	2002-06-05 01:41:04 BST	2002-06-05 01:41:04 BST	1364	Allocated	Allocated	unkn
00022.SPL				2002-06-05 01:41:04 BST	2002-06-05 01:41:04 BST	2002-06-05 01:41:03 BST	2002-06-05 01:41:03 BST	643244	Allocated	Allocated	unkn
FP00000.SHD				2002-06-05 01:00:58 BST	2002-06-05 01:00:58 BST	2002-06-05 01:00:58 BST	2002-06-05 01:00:58 BST	1344	Allocated	Allocated	unkn
FP00000.SPL				2002-06-05 01:00:58 BST	2002-06-05 01:00:58 BST	2002-06-05 01:00:57 BST	2002-06-05 01:00:57 BST	76616	Allocated	Allocated	unkn
00011.SPL				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unkn

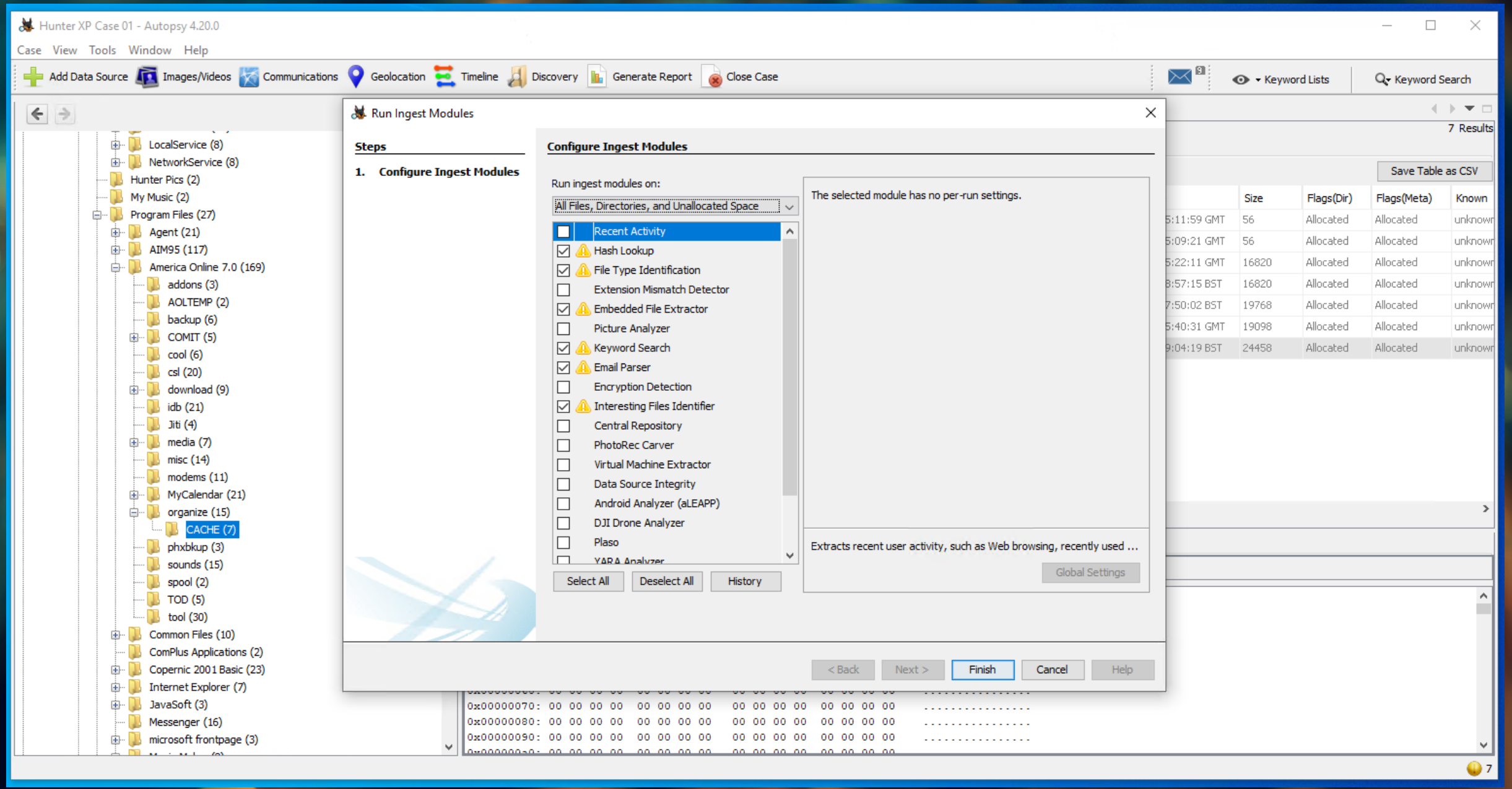
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Indexed Text | Translation

Page: 1 of 58 Page Go to Page: Script: Latin - Basic

∀Arial
∀Arial
∀Arial
∀Arial
Mr. Detsiwt, if you love your daughter you will E
∀Arial
click here!
∀Arial
∀Arial
wG !
xcdv


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
Agent (21)
AIM95 (117)
America Online 7.0 (169)
addons (3)
AOLTEMP (2)
backup (6)
COMIT (5)
cool (6)
csl (20)
download (9)
idb (21)
Jiti (4)
media (7)
misc (14)
modems (11)
MyCalendar (21)
organize (15)
CACHE (7)
phxbkup (3)
sounds (15)
spool (2)
TOD (5)
tool (30)
Common Files (10)
ComPlus Applications (2)
Copernic 2001 Basic (23)
Internet Explorer (7)
JavaSoft (3)
Messenger (16)
microsoft frontpage (3)
Listing
/img_Hunter XP.E01/vol_vol2/Program Files/America Online 7.0/organize/CACHE
7 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known
[current folder] 2002-05-14 19:04:19 BST 2002-05-14 19:04:19 BST 2002-06-05 00:27:54 BST 2002-03-01 15:11:59 GMT 56 Allocated Allocated unknown
[parent folder] 2002-03-01 15:58:10 GMT 2002-03-01 15:58:10 GMT 2002-06-05 00:27:54 BST 2002-03-01 15:09:21 GMT 56 Allocated Allocated unknown
ah1870 2002-03-01 15:40:31 GMT 2002-03-01 15:40:31 GMT 2002-03-01 15:40:31 GMT 2002-03-01 15:22:11 GMT 16820 Allocated Allocated unknown
ah1878 2002-05-14 18:57:15 BST 2002-05-14 18:57:15 BST 2002-05-14 18:57:15 BST 2002-05-14 18:57:15 BST 16820 Allocated Allocated unknown
chaser1100 2002-05-14 18:57:28 BST 2002-05-14 18:57:28 BST 2002-05-14 18:57:28 BST 2002-05-14 17:50:02 BST 19768 Allocated Allocated unknown
chaser1132 2002-05-14 17:49:33 BST 2002-05-14 17:49:33 BST 2002-05-14 17:49:33 BST 2002-03-01 15:40:31 GMT 19098 Allocated Allocated unknown
chaser1149 2002-06-05 01:48:30 BST 2002-06-05 01:48:30 BST 2002-06-05 01:48:30 BST 2002-05-14 19:04:19 BST 24458 Allocated Allocated unknown
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 2 Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000000: 41 4F 4C 56 4D 31 30 30 00 00 00 00 00 00 00 00 AOLVM100........
0x00000010: 34 11 00 00 00 08 00 00 00 02 01 00 00 00 00 00 4...............
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....


Hunter XP Case 01 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Run Ingest Modules
Steps
1. Configure Ingest Modules
Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Android Analyzer (aLEAPP)
DJI Drone Analyzer
Plaso
YARA Analyzer
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently used ...
Global Settings
< Back
Next >
Finish
Cancel
Help
7 Results
Save Table as CSV
Size
Flags(Dir)
Flags(Meta)
Known
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
Agent (21)
AIM95 (117)
America Online 7.0 (169)
addons (3)
AOLTEMP (2)
backup (6)
COMIT (5)
cool (6)
csl (20)
download (9)
idb (21)
Jiti (4)
media (7)
misc (14)
modems (11)
MyCalendar (21)
organize (15)
CACHE (7)
phxbkup (3)
sounds (15)
spool (2)
TOD (5)
tool (30)
Common Files (10)
ComPlus Applications (2)
Copernic 2001 Basic (23)
Internet Explorer (7)
JavaSoft (3)
Messenger (16)
microsoft frontpage (3)

Hunter XP Case 01 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

- LocalService (8)
- NetworkService (8)
- Hunter Pics (2)
- My Music (2)
- Program Files (27)
  - Agent (21)
  - AIM95 (117)
  - America Online 7.0 (169)
    - addons (3)
    - AOLTEMP (2)
    - backup (6)
    - COMIT (5)
    - cool (6)
    - csl (20)
    - download (9)
    - idb (21)
    - Jiti (4)
    - media (7)
    - misc (14)
    - modems (11)
    - MyCalendar (21)
    - organize (15)
      - CACHE (7)
    - phxbkup (3)
    - sounds (15)
    - spool (2)
    - TOD (5)
    - tool (30)
  - Common Files (10)
  - ComPlus Applications (2)
  - Copernic 2001 Basic (23)
  - Internet Explorer (7)
  - JavaSoft (3)
  - Messenger (16)
  - microsoft frontpage (3)

Listing

/img_Hunter XP.E01/vol_vol2/Program Files/America Online 7.0/organize/CACHE — 7 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2002-05-14 19:04:19 BST	2002-05-14 19:04:19 BST	2002-06-05 00:27:54 BST	2002-03-01 15:11:59 GMT	56	Allocated	Allocated	unknown
[parent folder]				2002-03-01 15:58:10 GMT	2002-03-01 15:58:10 GMT	2002-06-05 00:27:54 BST	2002-03-01 15:09:21 GMT	56	Allocated	Allocated	unknown
ah1870				2002-03-01 15:40:31 GMT	2002-03-01 15:40:31 GMT	2002-03-01 15:40:31 GMT	2002-03-01 15:22:11 GMT	16820	Allocated	Allocated	unknown
ah1878				2002-05-14 18:57:15 BST	2002-05-14 18:57:15 BST	2002-05-14 18:57:15 BST	2002-05-14 18:57:15 BST	16820	Allocated	Allocated	unknown
chaser1100				2002-05-14 18:57:28 BST	2002-05-14 18:57:28 BST	2002-05-14 18:57:28 BST	2002-05-14 17:50:02 BST	19768	Allocated	Allocated	unknown
chaser1132				2002-05-14 17:49:33 BST	2002-05-14 17:49:33 BST	2002-05-14 17:49:33 BST	2002-03-01 15:40:31 GMT	19098	Allocated	Allocated	unknown
chaser1149				2002-06-05 01:48:30 BST	2002-06-05 01:48:30 BST	2002-06-05 01:48:30 BST	2002-05-14 19:04:19 BST	24458	Allocated	Allocated	unknown

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Indexed Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text

```
6/3/2002    postmaster@guid        Delivery Status Notification (Failure)
6/3/2002    postmaster@guid        Delivery Status Notification (Failure)
6/3/2002    billyray150@hotm       here they are
6/3/2002    billyray150@hotm       Your Daughters Safety Depends on This!!!
<bearded gnomes> <stalking for dummies>
Error: Web Site Not Responding.
6/3/2002    billyray150@hotm       Re: Your Daughters Safety Depends on This!!!
6/3/2002    billyray150@hotm       If you love your daughter
Girls
6/3/2002    billyray150@hot        Re: Your Daughters Safety Depends on This!!!
6/3/2002    billyray150@hotm       Re: If you love your daughter
```

7

Hunter XP Case 01 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

Data Sources
- Hunter XP.E01_1 Host
  - Hunter XP.E01
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS / exFAT (0x07): 63-3318335)
      - $OrphanFiles (0)
      - $Extend (5)
      - $Unalloc (1)
      - AOL Instant Messenger (3)
      - Documents and Settings (7)
        - All Users (9)
        - Bob Hunter (18)
          - Application Data (7)
          - Cookies (41)
          - Desktop (12)
          - Favorites (14)
          - Local Settings (7)
            - Application Data (8)
            - History (4)
            - Temp (42)
            - Temporary Internet Files (4)
              - Content.IE5 (8)
                - 042WFPGU (505)
                - 6ZSJ6T6D (546)
                - 8XGPQD6L (603)
                - UFK38B83 (529)
          - My Documents (8)
          - NetHood (2)
          - PrintHood (2)
          - Recent (40)
          - SendTo (8)
          - Start Menu (4)
          - Templates (3)
          - WINDOWS (3)
        - Default User (98)
        - LocalService (8)

Listing | Keyword search 1 - getmsg

/img_Hunter XP.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83 — 529 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
getmsg[3]			0	2002-06-03 19:34:14 BST	2002-06-03 19:34:14 BST	2002-06-03 19:34:14 BST	2002-06-03 19:34:14 BST	4995	Allocated
getmsg[3].htm			0	2002-06-03 19:33:14 BST	2002-06-03 19:33:14 BST	2002-06-03 19:33:14 BST	2002-06-03 19:33:14 BST	24579	Allocated
getmsg[4]			0	2002-06-03 19:35:03 BST	2002-06-03 19:35:03 BST	2002-06-03 19:35:03 BST	2002-06-03 19:35:03 BST	4951	Allocated
getmsg[4].htm			0	2002-06-03 19:34:14 BST	2002-06-03 19:34:14 BST	2002-06-03 19:34:14 BST	2002-06-03 19:33:58 BST	24738	Allocated
getmsg[5].htm			0	2002-06-03 21:17:19 BST	2002-06-03 21:17:19 BST	2002-06-03 21:17:51 BST	2002-06-03 21:17:18 BST	21099	Allocated
getmsg[6].htm			0	2002-06-03 21:23:41 BST	2002-06-03 21:23:41 BST	2002-06-03 21:23:41 BST	2002-06-03 21:23:39 BST	21146	Allocated
getmsg[7].htm			0	2002-06-05 00:41:38 BST	2002-06-05 00:41:38 BST	2002-06-05 00:41:38 BST	2002-06-05 00:41:36 BST	25505	Allocated
getmsg[8].htm			0	2002-06-05 00:42:42 BST	2002-06-05 00:42:42 BST	2002-06-05 00:42:42 BST	2002-06-05 00:42:42 BST	5379	Allocated
global[1].js			0	2002-06-03 20:32:06 BST	2002-06-03 20:32:06 BST	2002-06-03 20:32:06 BST	2002-06-03 20:32:06 BST	7105	Allocated

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Download Images

chaser1191@hotmail.com
Save Address(es) Block — Previous Next | Close

From : "John Detsiwt" <John.Detsiwt@guidancesoftware.com>
To : <chaser1191@hotmail.com>
Subject : Bank Name, Account and Routing Numbers
Date : Mon, 3 Jun 2002 13:12:02 -0700

Reply Reply All Forward Delete Put in Folder... Printer Friendly Version

```
Bank of America
14921-24927
294812918

Please don't hurt her!
```

Calendar
Hotmail Services
Free Newsletters
MSN Featured Offers
POP Mail
Find Message
Reminders
Directories
Explore MSN
Free Games
Personals

Documenting findings

- The suspects appears to have been following two women.
- The women appear to be the daughters of a men named John and Ted.
- There is evidence of extortion being made regarding the safety of this woman if payment is not received

Do you think this is enough to make a solid case?

Do you think there might be additional evidence to be found from further analysis of the disk image?

Anti-forensics

In scenarios where the potential criminal is aware of digital forensics, they may take steps to conceal data or prevent an investigation from being able to produce evidence.

Examples of anti-forensics:

- Artifact wiping – removing files and data from the system forensically
- Encryption – making the data unreadable without the key
- Steganography – hiding secret information in a manner where it is difficult to establish it's even present


Any Questions?
Thank You