When anyone is fired

What do you do when an employee quits and/or goes to work for the competitor.

Human Resources

What is your company's policy:

- When an employee quits
- When an employee is fired

Human Resources

Are you an inside network Administrator or an outside Administrator?

Human Resources

- Most of the time you are at the mercy of the people you work for.
- Talk with them.
- Explain to them that you have to be informed on anyone living the company as soon as possible.

Ex-employee

- What rights did that ex-employee have?
- Where is his/her profile?
- Does he/she have a backup drive or folders on the server?
- Where is his/her email kept?

Ex-employee

- Does he/she have excess to the network from an outside source?
- Does he/she have excess to the company internet or intranet?
- Does he/she have excess to other third party programs (training, sales, finance, etc.)?

What to do with the Ex-employee's Stuff

- This is always a hard question to answer.
- If you work for a large company that has a lot of employee turn over, what to do?
- If you are a small company, what to do?
- If you are outside contract, what to do?

Large Companies

- Most large companies, (Micron, Albertsons, Hewlett Packard, etc., they already have people trained in computer forensics.
- They also have to deal with e-Discovery.
- Most large companies already have computer forensics enterprise programs.

eDisovery

- Electronic discovery (also called e-discovery or eDiscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent and/or network of using it as evidence in a civil or criminal legal case.

eDiscovery

- eDiscovery is usually easier than the normal computer forensic examination.
- Your knot usually looking for what someone is hiding.
- You are mostly look for allocated files and not deleted/overwritten items unless the attorney is asking for that.

From Wikipedia

- **Electronic discovery**, or "e-discovery", refers to discovery in civil litigation which deals with information in *electronic form*. In this context, *electronic form* is the representation of information as binary numbers. Electronic information is different from paper information because of its intangible form, volume, transience, and persistence. Also, electronic information is usually accompanied by metadata,

From Wikipedia

- which is rarely present in paper information. Electronic discovery poses new challenges and opportunities for attorneys, their clients, technical advisors, and the courts, as electronic information is collected, reviewed and produced. Electronic discovery is the subject of amendments to the Federal Rules of Civil Procedure which are effective December 1, 2006.

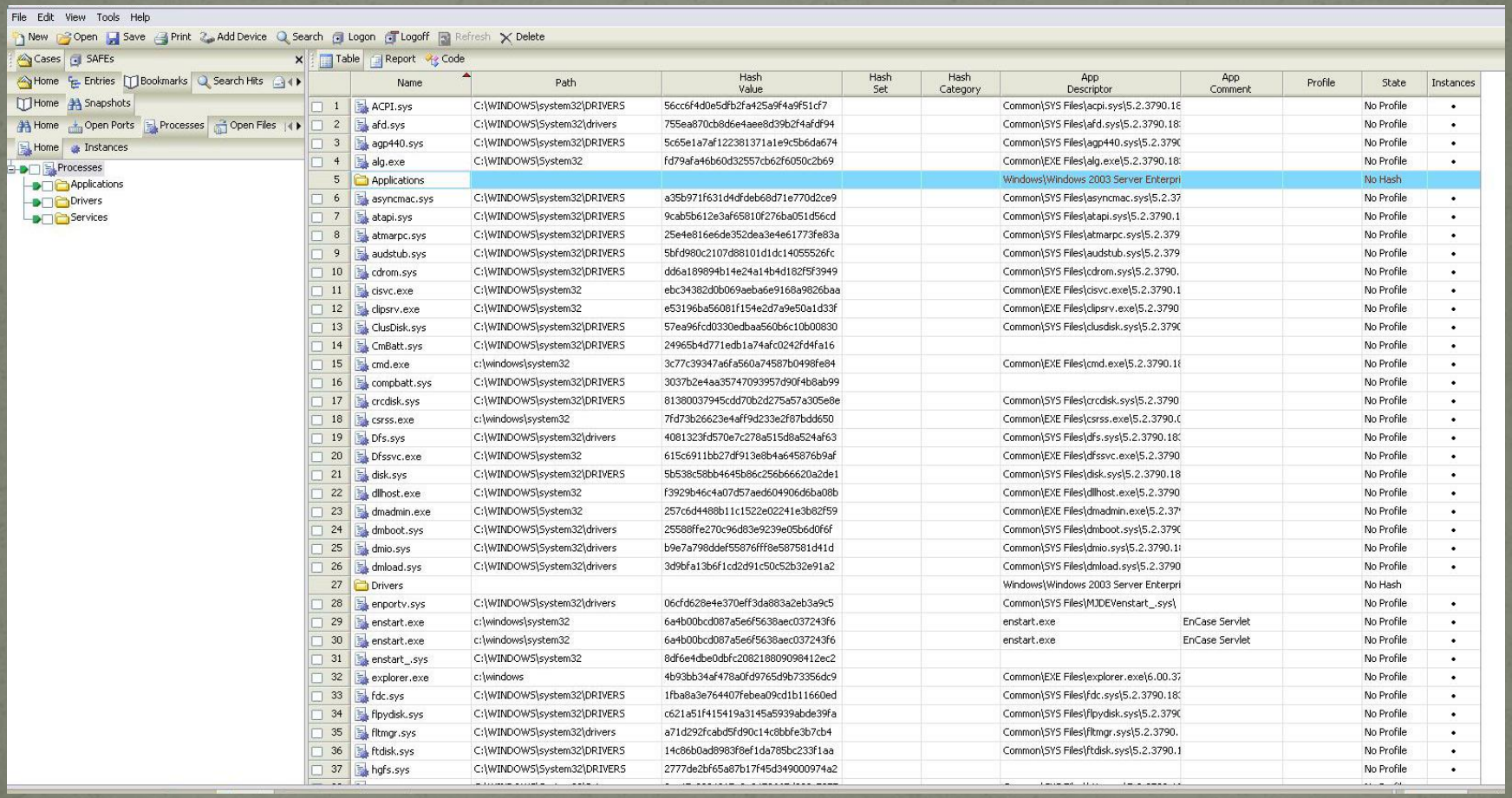
eDiscovery

- Normally you are looking for documents and e-mails.
- The attorney or court will give you a list of text searches and search for those items only.
- Normally you are searching over a large amount of computers.

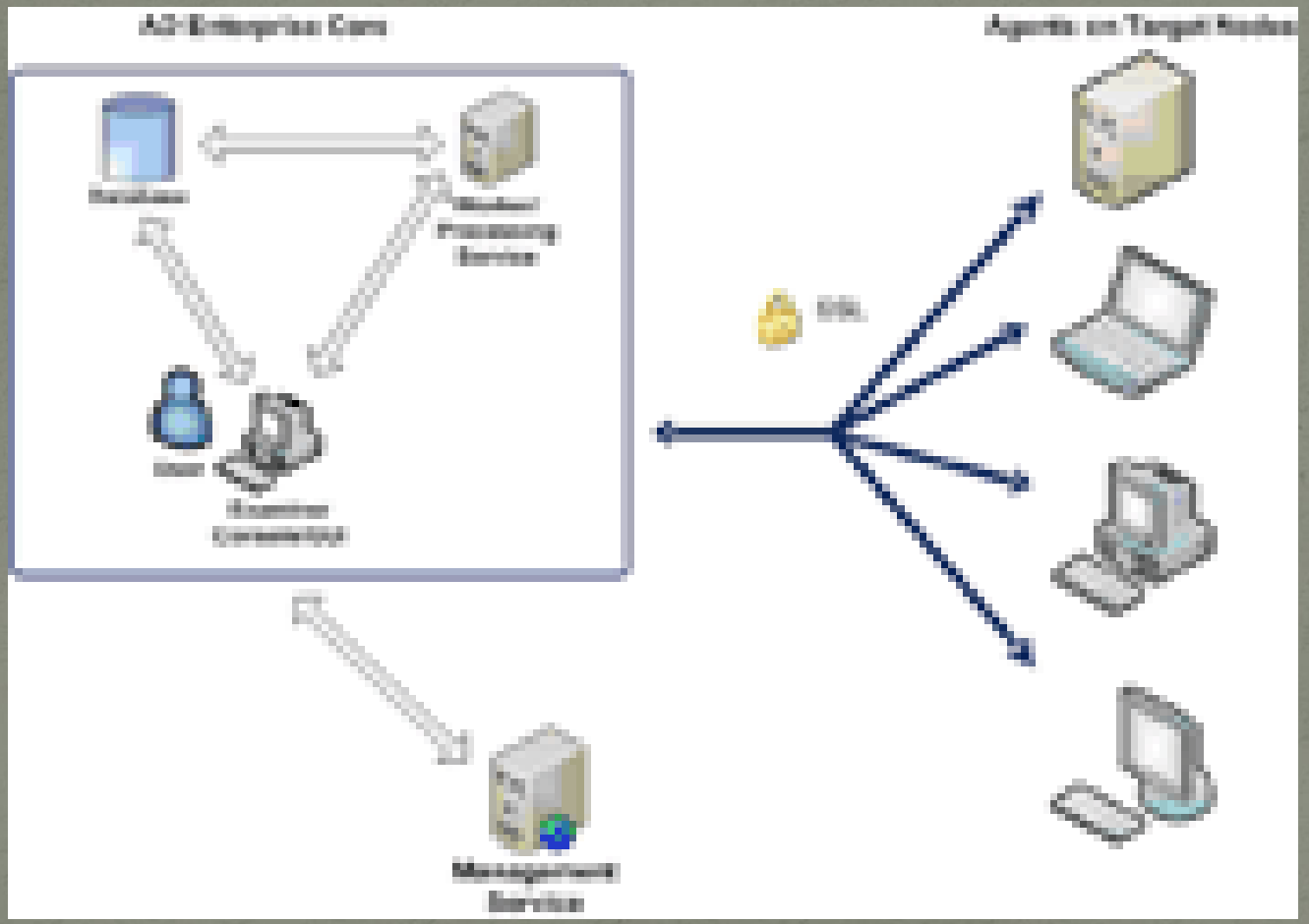
Software for eDiscovery

- **EnCase Enterprise**
- **AccessData Enterprise**
- **Wetstone's LiveDiscover™ Forensic Edition- Live Forensic Discovery**
- **Cyber Security Technologies OnLineDFS**

EnCase® Enterprise



AccessData Enterprise



LiveDiscover™ Forensic Edition- Live Forensic Discovery

- Live forensic network mapping
- Live forensic vulnerability assessment

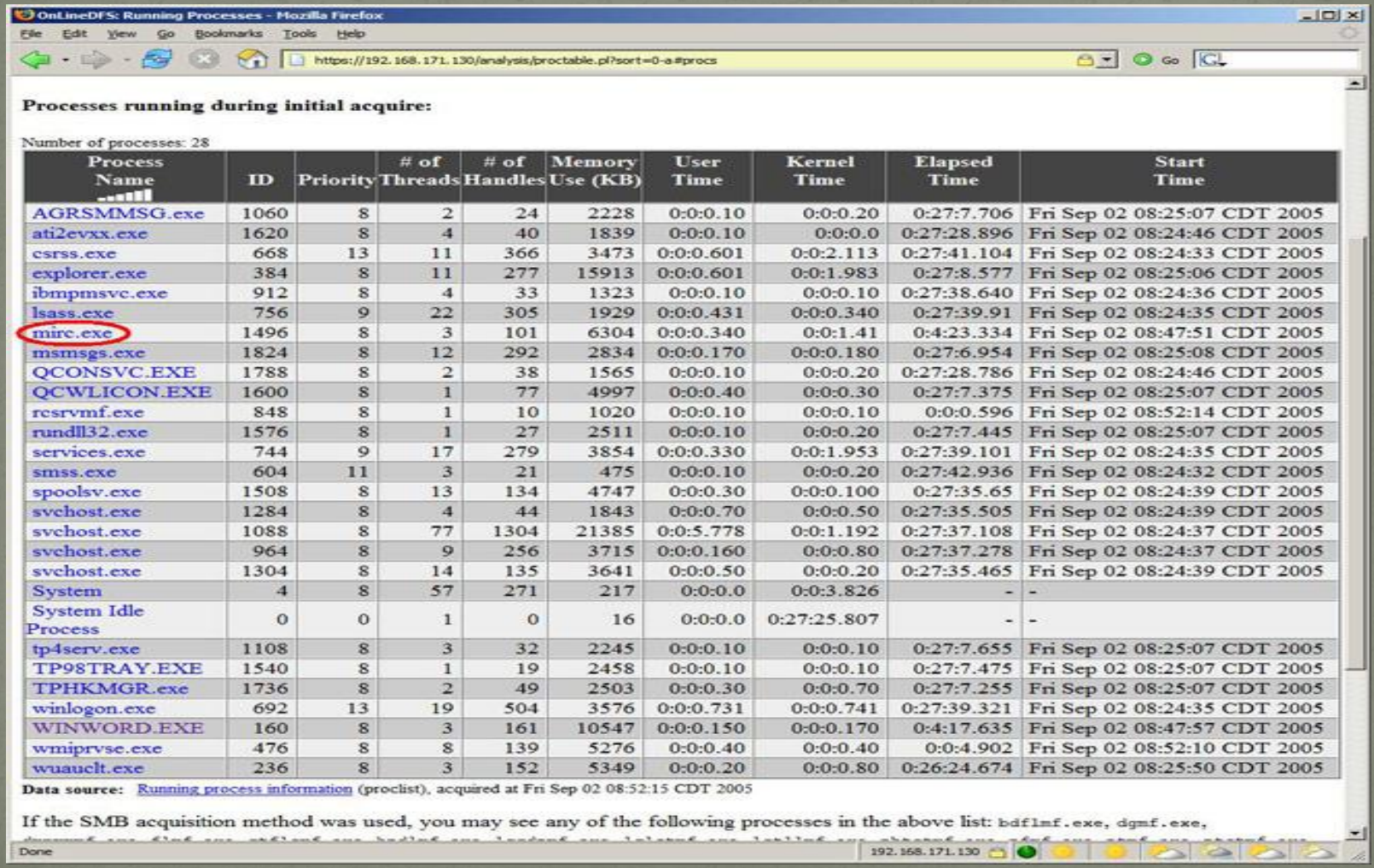
- Live capturing of system information including:

- IP addresses
- MAC addresses
- System type
- System name
- Operating system information
- User account information
- Running services
- Network devices
- Computer/network shares

LiveDiscover™ Forensic Edition- Live Forensic Discovery

- Recognizes Windows, Unix, Linux, Macintosh, VMS, Novell, OS/2, and Sun operating systems and much more
- Forensically maps workstations, servers, switches, CD servers, jukeboxes, online storage, etc.
- Investigator tailored easy to read graphs and reports, with a user interface that is intuitive and easy to understand
- Modify or add custom vulnerability scripts, making LiveDiscover FE extensible
- Receive e-mail when an extensive system scan identifies critical information
- Remote detection of system status including running services, attached devices, printers and more
- Forensic detailed report generation

OnLineDFS



OnLineDFS: Running Processes - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.171.130/analysis/proctable.pl?sort=0-a#procs

Processes running during initial acquire:

Number of processes: 28

Process Name	ID	Priority	# of Threads	# of Handles	Memory Use (KB)	User Time	Kernel Time	Elapsed Time	Start Time
AGRSMMSG.exe	1060	8	2	24	2228	0:0:0.10	0:0:0.20	0:27:7.706	Fri Sep 02 08:25:07 CDT 2005
ati2evxx.exe	1620	8	4	40	1839	0:0:0.10	0:0:0.0	0:27:28.896	Fri Sep 02 08:24:46 CDT 2005
csrss.exe	668	13	11	366	3473	0:0:0.601	0:0:2.113	0:27:41.104	Fri Sep 02 08:24:33 CDT 2005
explorer.exe	384	8	11	277	15913	0:0:0.601	0:0:1.983	0:27:8.577	Fri Sep 02 08:25:06 CDT 2005
ibmpmsvc.exe	912	8	4	33	1323	0:0:0.10	0:0:0.10	0:27:38.640	Fri Sep 02 08:24:36 CDT 2005
lsass.exe	756	9	22	305	1929	0:0:0.431	0:0:0.340	0:27:39.91	Fri Sep 02 08:24:35 CDT 2005
mirc.exe	1496	8	3	101	6304	0:0:0.340	0:0:1.41	0:4:23.334	Fri Sep 02 08:47:51 CDT 2005
msmsgs.exe	1824	8	12	292	2834	0:0:0.170	0:0:0.180	0:27:6.954	Fri Sep 02 08:25:08 CDT 2005
QCONSVC.EXE	1788	8	2	38	1565	0:0:0.10	0:0:0.20	0:27:28.786	Fri Sep 02 08:24:46 CDT 2005
QCWLICON.EXE	1600	8	1	77	4997	0:0:0.40	0:0:0.30	0:27:7.375	Fri Sep 02 08:25:07 CDT 2005
rcsrvmf.exe	848	8	1	10	1020	0:0:0.10	0:0:0.10	0:0:0.596	Fri Sep 02 08:52:14 CDT 2005
rundll32.exe	1576	8	1	27	2511	0:0:0.10	0:0:0.20	0:27:7.445	Fri Sep 02 08:25:07 CDT 2005
services.exe	744	9	17	279	3854	0:0:0.330	0:0:1.953	0:27:39.101	Fri Sep 02 08:24:35 CDT 2005
smss.exe	604	11	3	21	475	0:0:0.10	0:0:0.20	0:27:42.936	Fri Sep 02 08:24:32 CDT 2005
spoolsv.exe	1508	8	13	134	4747	0:0:0.30	0:0:0.100	0:27:35.65	Fri Sep 02 08:24:39 CDT 2005
svchost.exe	1284	8	4	44	1843	0:0:0.70	0:0:0.50	0:27:35.505	Fri Sep 02 08:24:39 CDT 2005
svchost.exe	1088	8	77	1304	21385	0:0:5.778	0:0:1.192	0:27:37.108	Fri Sep 02 08:24:37 CDT 2005
svchost.exe	964	8	9	256	3715	0:0:0.160	0:0:0.80	0:27:37.278	Fri Sep 02 08:24:37 CDT 2005
svchost.exe	1304	8	14	135	3641	0:0:0.50	0:0:0.20	0:27:35.465	Fri Sep 02 08:24:39 CDT 2005
System	4	8	57	271	217	0:0:0.0	0:0:3.826	-	-
System Idle Process	0	0	1	0	16	0:0:0.0	0:27:25.807	-	-
tp4serv.exe	1108	8	3	32	2245	0:0:0.10	0:0:0.10	0:27:7.655	Fri Sep 02 08:25:07 CDT 2005
TP98TRAY.EXE	1540	8	1	19	2458	0:0:0.10	0:0:0.10	0:27:7.475	Fri Sep 02 08:25:07 CDT 2005
TPHKMGR.exe	1736	8	2	49	2503	0:0:0.30	0:0:0.70	0:27:7.255	Fri Sep 02 08:25:07 CDT 2005
winlogon.exe	692	13	19	504	3576	0:0:0.731	0:0:0.741	0:27:39.321	Fri Sep 02 08:24:35 CDT 2005
WINWORD.EXE	160	8	3	161	10547	0:0:0.150	0:0:0.170	0:4:17.635	Fri Sep 02 08:47:57 CDT 2005
wmiprvse.exe	476	8	8	139	5276	0:0:0.40	0:0:0.40	0:0:4.902	Fri Sep 02 08:52:10 CDT 2005
wuauclt.exe	236	8	3	152	5349	0:0:0.20	0:0:0.80	0:26:24.674	Fri Sep 02 08:25:50 CDT 2005

Data source: Running process information (proclist), acquired at Fri Sep 02 08:52:15 CDT 2005

If the SMB acquisition method was used, you may see any of the following processes in the above list: bdflmf.exe, dgmf.exe,

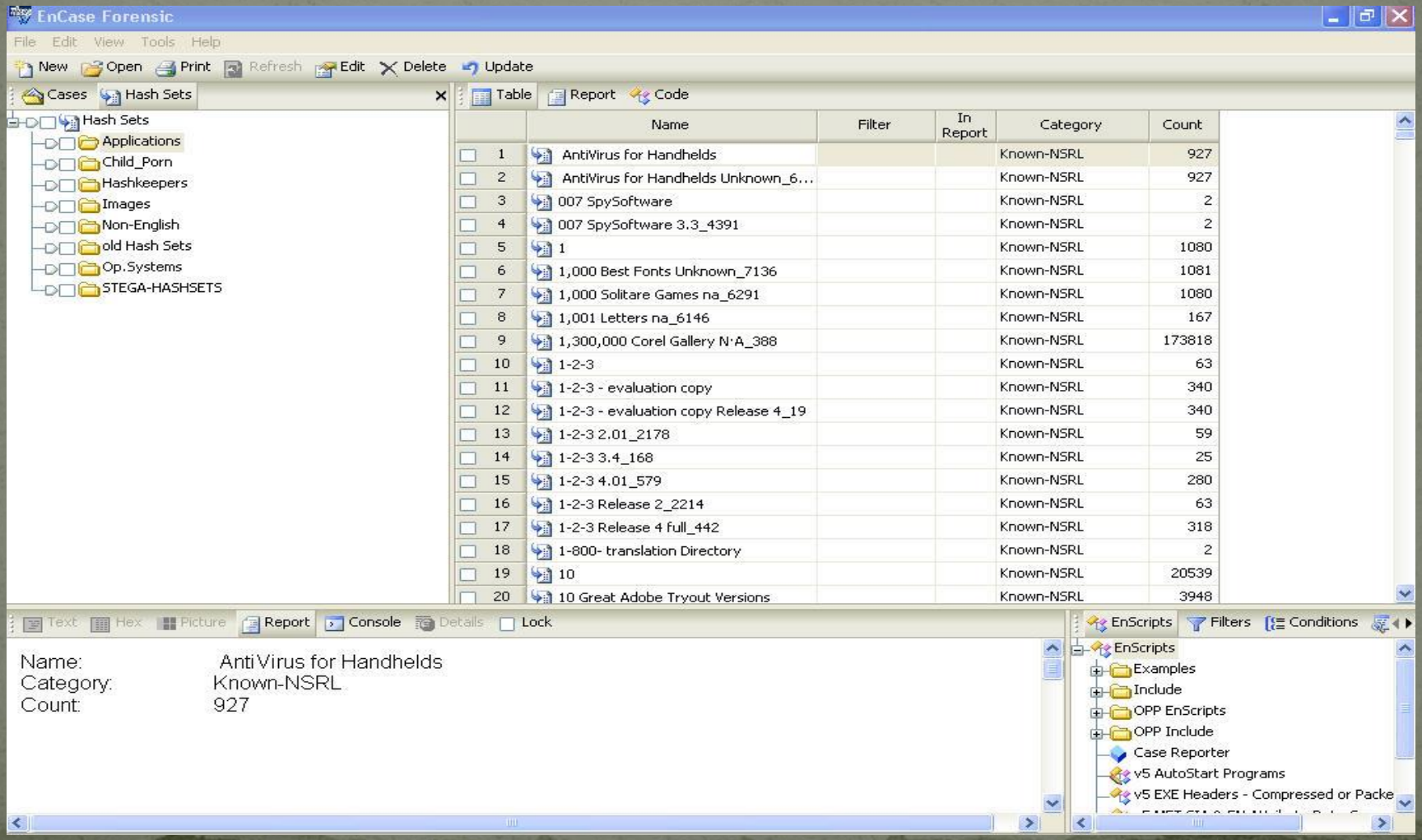
Done

192.168.171.130

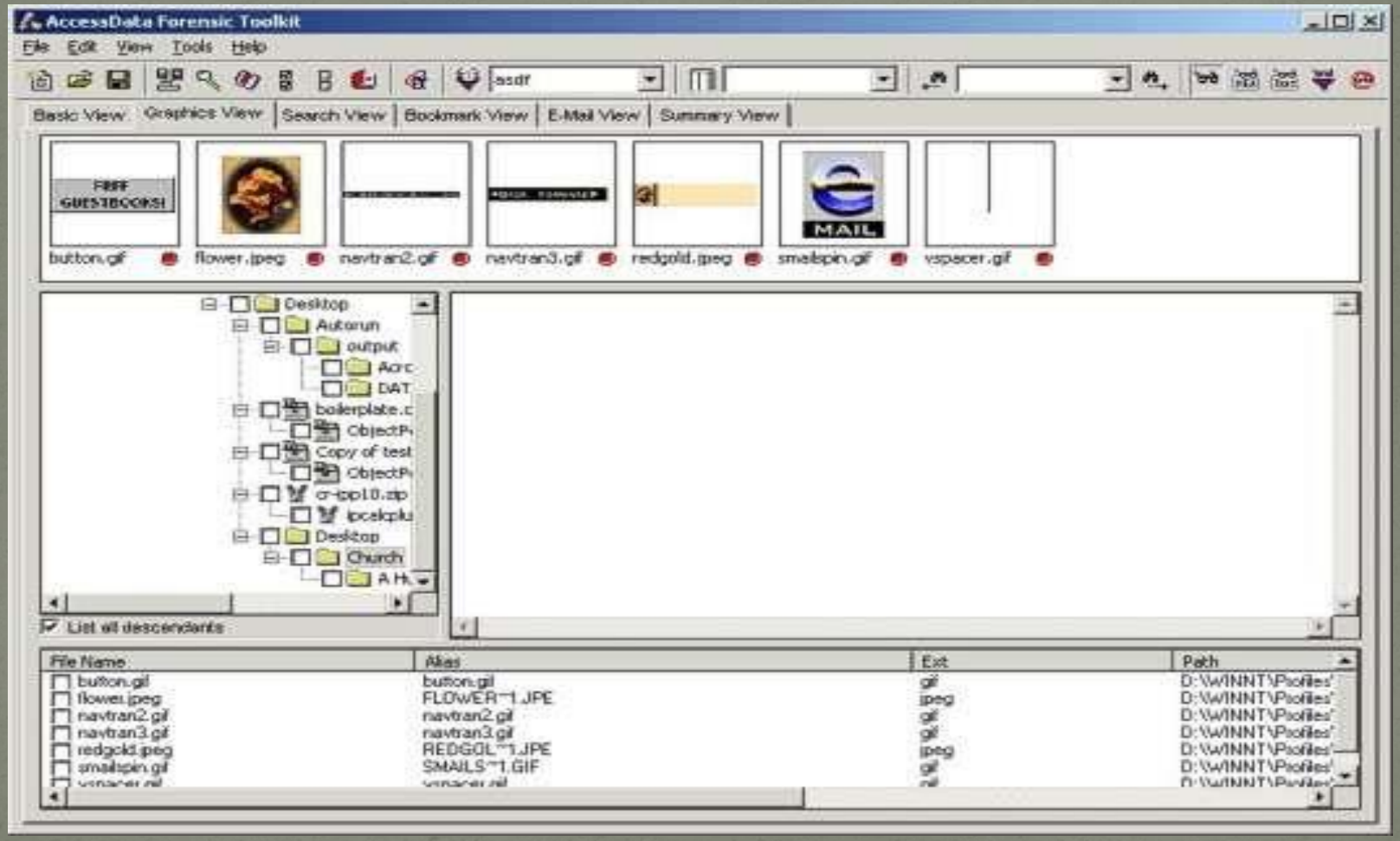
Computer Forensic Software

- **EnCase**
- **Forensic Tool Kit**
- **X-Ways**
- **Forensic Explorer**

Guidance Software's EnCase



Accessdata's Forensic Toolkit



X-Ways

X-Ways Software Technology AG

Deutsch
Français
Español

Orders, Prices:
- Credit card
- Wire transfer or check

Products

Services

Contact X-Ways
Support forum

Corporate info

Products

X-Ways Forensics	Integrated computer forensics environment Our flagship product, based on WinHex
WinHex	Computer forensics, data recovery, and IT security tool Hex editor, disk editor, and RAM editor
X-Ways Capture	*Successfully* seize all media, files, and RAM from Windows+Linux live systems
Davory	Data recovery made *easy*
Evidor	Forensic keyword search tool, focus on ease of use
X-Ways Trace	User activity deciphered
X-Ways Replica	Forensically sound hard disk cloning & imaging under DOS
X-Ways Security	Permanent erasure

If nothing else

- Write down the date and time from the BIOS.
- Remove hard drive
- Store in locked safe place.

If nothing else

- Backup Tapes with Profiles
- Exchange Server (file headers for e-mail)

What G2 Research do the most of

- Wrongful termination suits
  - Employee is fired, six months later sues
  - Network Systems people add new user on same computer or ghost new image onto computer.
- Theft of trade secrets
  - Employee quits and goes to work for competitor, taking all of his past work papers
  - Sometimes employee hacks into his old company and downloads all the data he can find

What should IT do

- When a employee leaves get them out of the network system asap
- Image the hard drive or remove it from the computer. Write down the computer's date and time and label the employees hard drive or image. Hard drives are cheaper than the law suit.