Investigator's Office, Laboratory, & Forensic Certification

Nelson Chapter 2

plus

Additional material

Topics in this Lecture

Administrative Items

Forensic Imaging Lab (from last week)
Assign02b_c

WinHex File Forensics Lab (cleaning a JPEG image)
Assign03a_rds

Uniform Crime Reports

Computer forensic investigator certification

Computer forensic laboratory certification

Internet Crime Complaint Center (IC^3)

Computer forensics laboratories

Forensic Workstation

Business Case for Developing a Forensics Lab

Administrative Items

Assignments and RADISH

Assignments

No late assignments are accepted

After due date, assignment can no longer be submitted

If you have issues, you MUST notify me PRIOR to the due date

Assignments are no longer visible 24 hours after the due date

RADISH was down over the weekend

Be sure you fill out the support form (Google Forms) that was provided to you in your initial RADISH email

Send me email right afterwards to let me know you are having issues

Keep up-to-date with the course

Know when assignments are due

Monitor your email for messages from me, Phil or ForSecLab

Go to Blackboard and view announcements

Forensic Imaging Lab

Forensic Imaging Lab Outline

In this lab, we will make forensic copies of a disk image

Image location:

R:\share\Labs\Chapter1\Ch01InChap01.dd

General outline of lab:

Copy over image to your E: drive

Use certutil Windows command line tool to determine hashes

Create and verify forensic copy using WinHex

Create and verify forensic copy using FTKImager

You will follow along during class. Be sure to take screenshots along the way (I will remind you) as you will submit your results of this lab via *Assign02b_s*.

WinHex File Forensics Lab

WinHex File Forensics Lab

WinHex Configuration

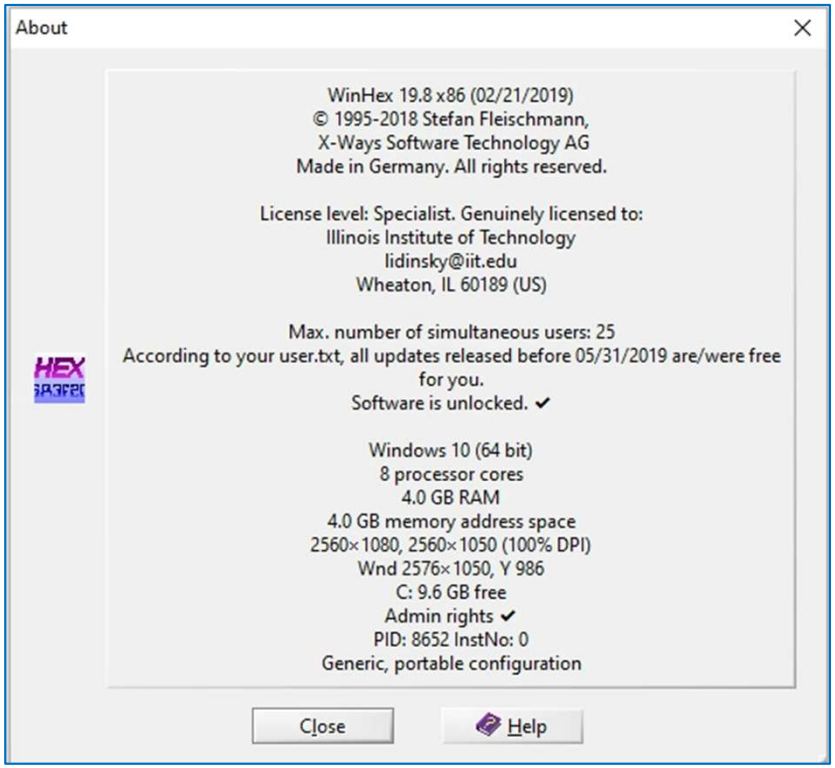
Log onto RADISHng

Open your *Windows Cyber Forensics (ITMS 538 Windows)* desktop

Open WinHex, using the Windows menu

You will likely be greeted with the About… splash screen

Click "Close"



WinHex File Forensics Lab

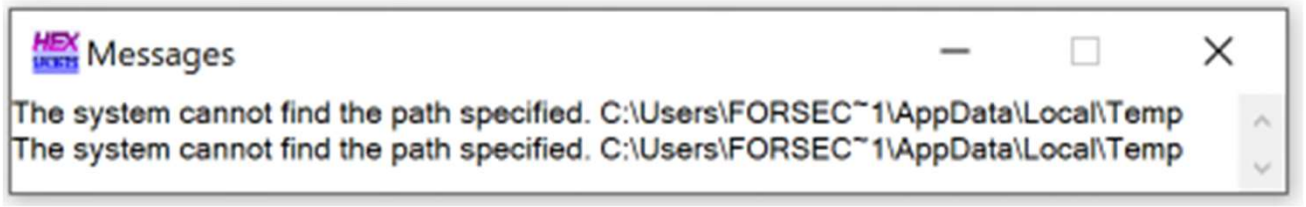
WinHex Configuration

Log onto RADISHng

Open your *Windows Cyber Forensics (ITMS 538 Windows)* desktop

Open WinHex, using the Windows menu

Note that you will get the following messages once WinHex opens



This indicates that we need to change some settings…

WinHex File Forensics Lab

WinHex Configuration

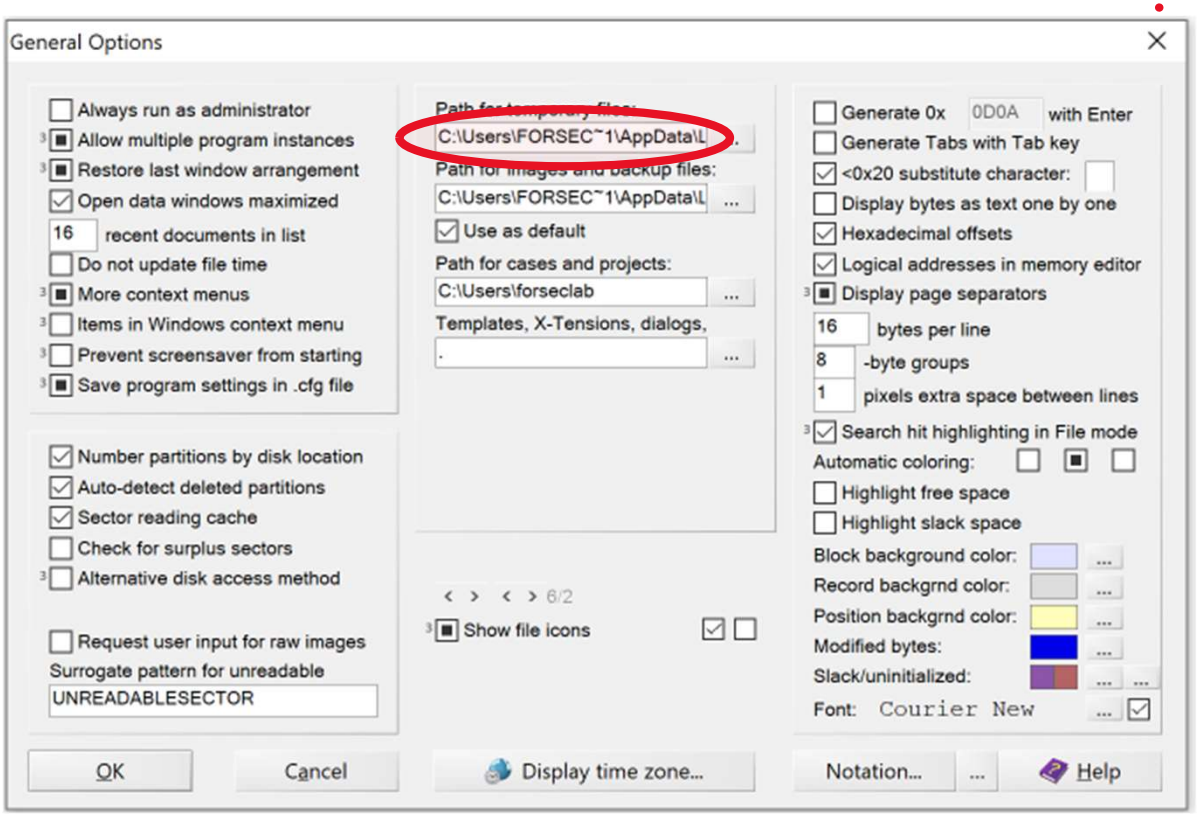
Close the Messages window

Select the Options > General… menu item

WinHex File Forensics Lab

WinHex Configuration

Click “Path for temporary files:” text box to enable it for editing



WinHex File Forensics Lab

WinHex Configuration

Change the path in the textbox from:

C:\Users\FORSEC~1\AppData\Local\Temp

to

C:\Users\<your user name>\AppData\Local\Temp

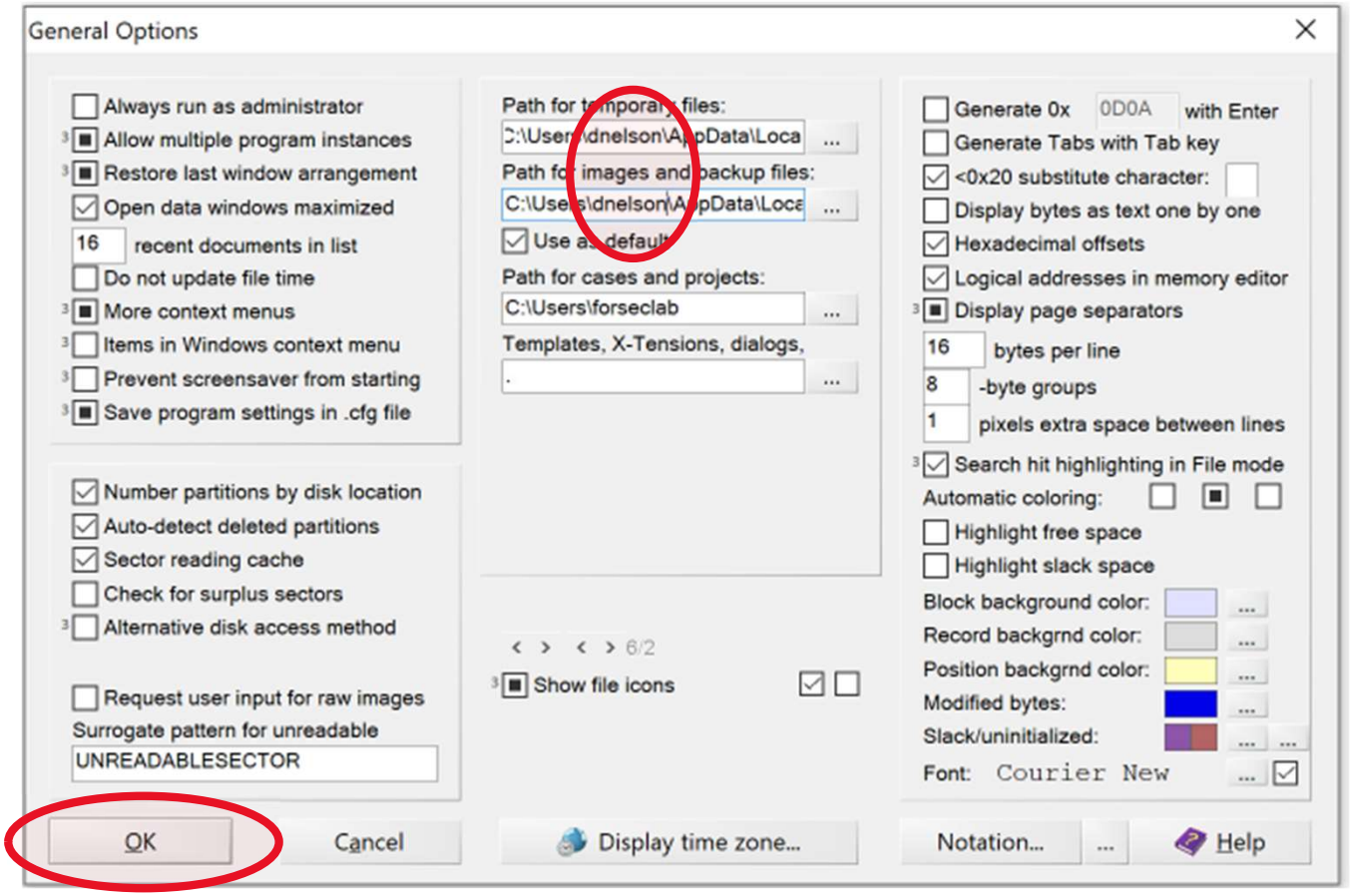
(The change you need to make is highlighted in red text.)

Make the same change in the "Path for images and backup files:" textbox

WinHex File Forensics Lab

WinHex Configuration

Click “OK”



WinHex File Forensics Lab

WinHex Configuration

To confirm that this issue has been resolved:

Exit from WinHex

Start up WinHex

Verify that you no longer get the messages shown on slides 3 and 4.

WinHex File Forensics Lab

JPEG Files

From the ***Nelson*** text:

> *"All JPEG files, including Exif, start from offset 0 (the first byte of a file) with hexadecimal FFD8. The current standard header for regular JPEG files is JPEG File Interchange Format (JFIF), which has the hexadecimal value FFE0 starting at offset 2… In addition, the hexadecimal values at offset 6 specify the label name [in our case JFIF]."*

So, JPEG files with label "JFIF" should start out with the following hexadecimal sequence:

file offset	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
value	FF	D8	FF	E0	00	10	4A	46	49	46
							J	F	I	F

WinHex File Forensics Lab

JPEG Files

On your RADISHng Windows 10 Desktop:

In the File Explorer, go to the following directory:

R:\share\Labs\WinHex Lab

Copy the following file to your Documents directory:

clownFish-corrupted.jpg

Try to open this image file

Was it successful?

WinHex File Forensics Lab

JPEG Files

In WinHex:

Select the following menu item: File > Open…

Open the clownFish-corrupted.jpg file in your Documents directory

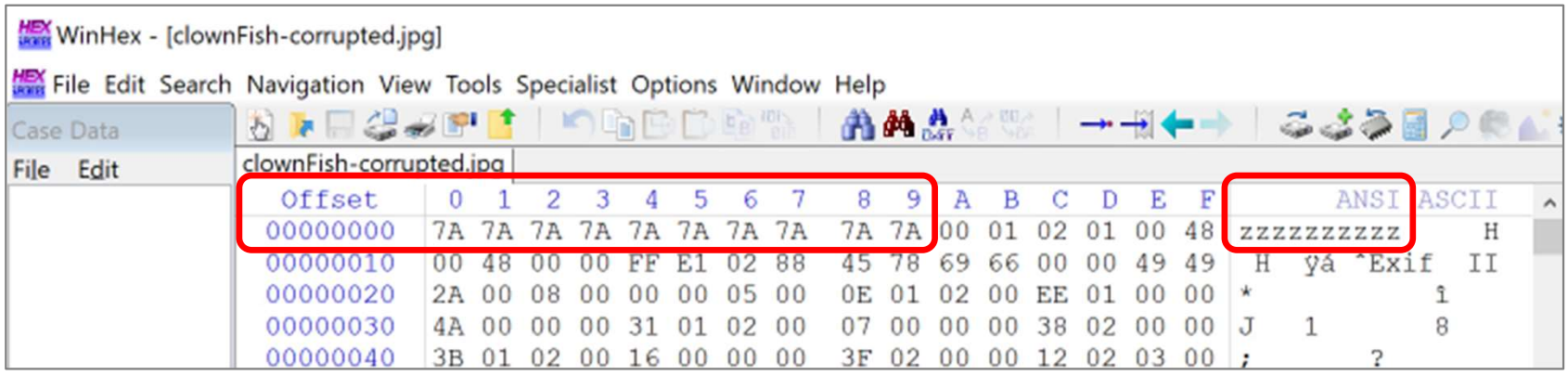
WinHex File Forensics Lab

Clean up clownFish JPEG file

Recall that the beginning of a JPEG file with a label of "JFIF" should begin as:

file offset	0	1	2	3	4	5	6	7	8	9
value	FF	D8	FF	E0	00	10	4A	46	49	46
							J	F	I	F

However, the clownFish-corrupted.jpg file starts with all "z"'s (note that 7A in hexadecimal is "z" in ASCII text)



WinHex File Forensics Lab

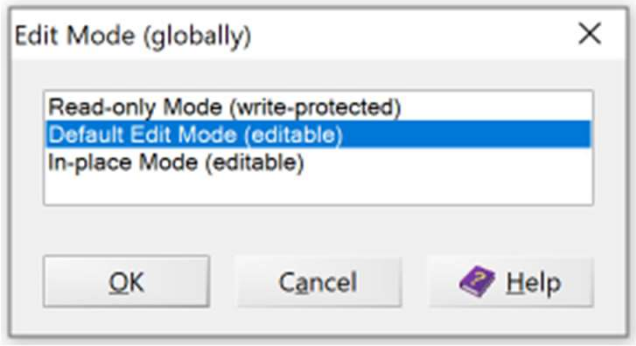
Clean up clownFish JPEG file

We'll now "clean" this file by overwriting the errant bytes

In WinHex, go into Edit mode by selecting the following menu item:

Options > Edit Mode…

A pop-up window will appear. Choose "Default Edit Mode"



Click "OK"

WinHex File Forensics Lab

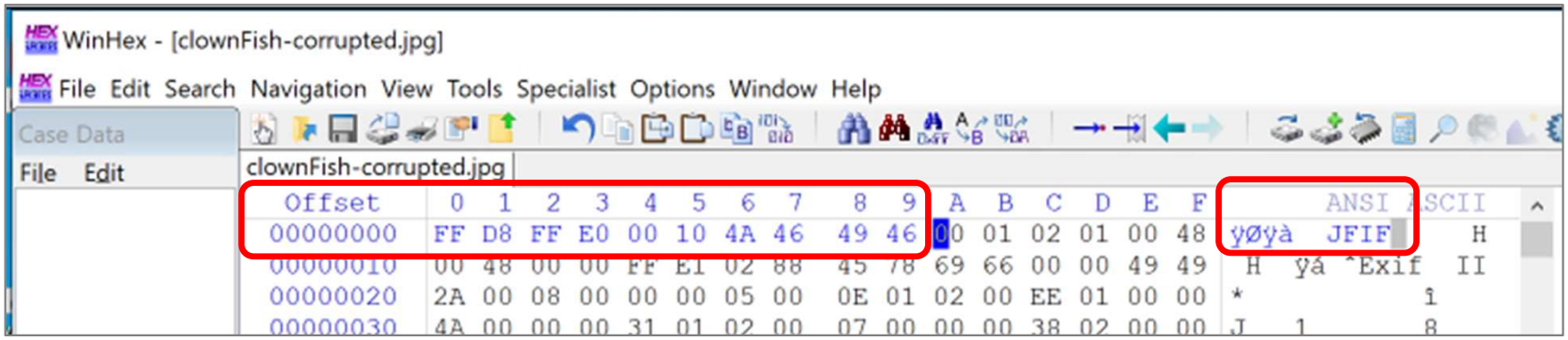
Clean up clownFish JPEG file

Overwrite the first 9 bytes of the clownFish-corrupted.jpg file with the correct byte sequence as shown below

(Be sure to edit the hexadecimal values):

file offset	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
value	FF	D8	FF	E0	00	10	4A	46	49	46
							J	F	I	F

The first 9 bytes should now look like this:



WinHex File Forensics Lab

Save and Verify Your Cleaned clownFish JPEG file

In WinHex:

Select the following menu item in WinHex:

File > Save As…

Save this file with the following name in your Documents directory:

clownFish-clean.jpg

Exit WinHex

Verify that the JPEG image has been cleaned/repaired:

Using the File Explorer, go to your Documents folder

Open the clownFish-clean.jpg file by double-clicking on it

WinHex File Forensics Lab

Save and Verify Your Cleaned clownFish JPEG file

Verify that you see the image of a clownfish:

WinHex File Forensics Lab

Assign03a_s and Assign03b_rds

The lab we just performed should provide the necessary background to complete the Assign03a_s assignment

- *You have to clean a file*
- *The file you clean is the next assignment (Assign03b_rds)*
- *You will have to submit your cleaned file along with an explanation of the steps you used to repair the file*

Assign03b_rds

- *You have to complete Assign03a_s to start Assign03b_rds*
- *Involves reading assignments (rd) and submittal (s)*
- *Submit your answers in one document*

Terminology

Imprecise Terminology

There are several terms that are used imprecisely

Network Forensics

Investigation of criminal, civil & administrative violations involving communications networks including both voice and computer networks

Computer Forensics

Investigation of crimes, civil & administrative violations involving computers

Clearly there is overlap between the two terms

Increasingly the literature uses **Cyber Forensics** to mean both together

Imprecise Terminology

High Tech Forensics

Subsumes computer and network forensics

Increasingly referred to as ***cyber forensics***

But also can include other sciences

DNA testing

Infrared and RF surveillance

...

Computer Forensic Laboratories

Where?

Forensic analysis should be done in the laboratory

Doing it at home is sometimes difficult because

- Often bit-stream copying and follow-on analysis takes days
- Chain of custody can be suspect unless precautions are taken
- In the case of criminal or civil crimes, home may not meet acceptable security standards

Preliminary analysis can sometimes be done at the scene with proper tools and procedures

Portable forensic workstation (e.g., FREDDIE)

Sealed-off and guarded site

…

Lab Management

Per ASCLD, lab management must document that they do specific things and run the lab according to a set of ASCLD guidelines:

Set up the guidelines for managing cases

Promote group consensus for decision making

Establish and promote quality assurance

Create and monitor lab policies

Evaluate hardware and software needs

Balance costs and needs

Laboratory Should Be Secure

Floor-to-ceiling walls

Avoid windows if possible

Controlled access

Lockable

Log for all visitors

Possibly log for all personnel

Trash containers for two or more separate types of trash

Anti-static carpets and/or floor pads

Evidence Locker

Separate evidence locker within the lab

Lockable heavy-duty cabinet or separate lockable room

Log all movement of material in and out of locker

Chain of custody

Limit number of people (custodians) with access to the locker to a subset of those with access to the lab

Forensic examiners must go through custodians to check in and check out evidence

Evidence containers should be locked when they are not under the immediate supervision of an authorized person

Evidence Locker
Combination Locks

Provide the same level of security for the combination as for the content of the evidence containers

Destroy any previous combinations after setting up a new combination

Allow only a very limited number of authorized personnel to change lock combinations

Not all the custodians

Change the lock combinations every six months and when an authorized person leaves the organization

Evidence Locker
Key Locks

Appoint a key custodian responsible for distributing keys

Stamp identification, “do not reproduce” message and sequential numbers on each duplicate key

Maintain a registry listing the assigned keys

Conduct a monthly audit to ensure no keys were lost

Take an inventory of all keys

Leave the keys in the lab

Change locks and keys annually or when a key is lost

Do **not** use a master key for several locks

High-risk Investigations

- High-risk Crimes
  - *e.g., National security*
    - *Murder*
- Might require more than minimum forensic lab requirements
- Greater challenges to keep investigation secure
  - *Network Transmissions*
  - *Electromagnetic radiation (EMR)*
    - Computers emanate radiation
    - Equipment exists today that can sense computer and display radiation from 10s to 100s of meters away

High-risk Investigations

A forensic lab that meets the needs of high-risk investigations needs to limit or contain EMR

U.S. Dept. of Defense has defined a facility that does this

Called "TEMPEST"

www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981

Tempest-Qualified Lab

Filtered uninterruptible electrical power

A “screen room”

RF shielding in walls, ceiling and floor (Often this takes the form of copper screen.)

Low radiation monitors and computers

Heating & AC ducts need special baffles to block RF and sound

Tempest-Qualified Lab

"Lock-room" entry/exit

Entry is through 2 doors with an anteroom between them

Doors have metal moldings for RF shielding

Doors are interlocked

Cannot have both doors open at same time

Often the anteroom has some additional form of security that limits entry and exit

Conducting High-Risk Investigations

TEMPEST facilities are very expensive

It may be sufficient to use low-emanation workstations instead

Lab Communications

High bit rate always-on Internet access

Alternate Internet access should also be available as a backup

But the forensic workstations should **not** be attached to the Internet

Maybe a separate LAN for the forensic workstations and NAS *(Network Attached Storage)*

Not connected to the Internet or

A LAN that can be physically disconnected from the Internet

Mechanical & Electronic Capabilities

Lab should have the ability to mechanically assemble and disassemble computers & computer components

Need workbench and tools

Electronic test equipment desirable

Multimeters

Logic analyzer

Oscilloscope?

…

Helpful to be able to microscopically look at things

Reference Materials

Library of reference material

- *Software manuals*
- *Hardware manuals*
- *Forensic literature*

Determining Floor Plans for a Forensic Lab

How you configure the work area will depend on:

- *Your budget*
- *Amount of available floor space*
- *Number of computers you assign to each computing investigator*

Ideal configuration is to have:

- *Two forensic workstations*
- *One non-forensic workstation with Internet access*

Small or Home-Based Lab

Small labs usually consist of

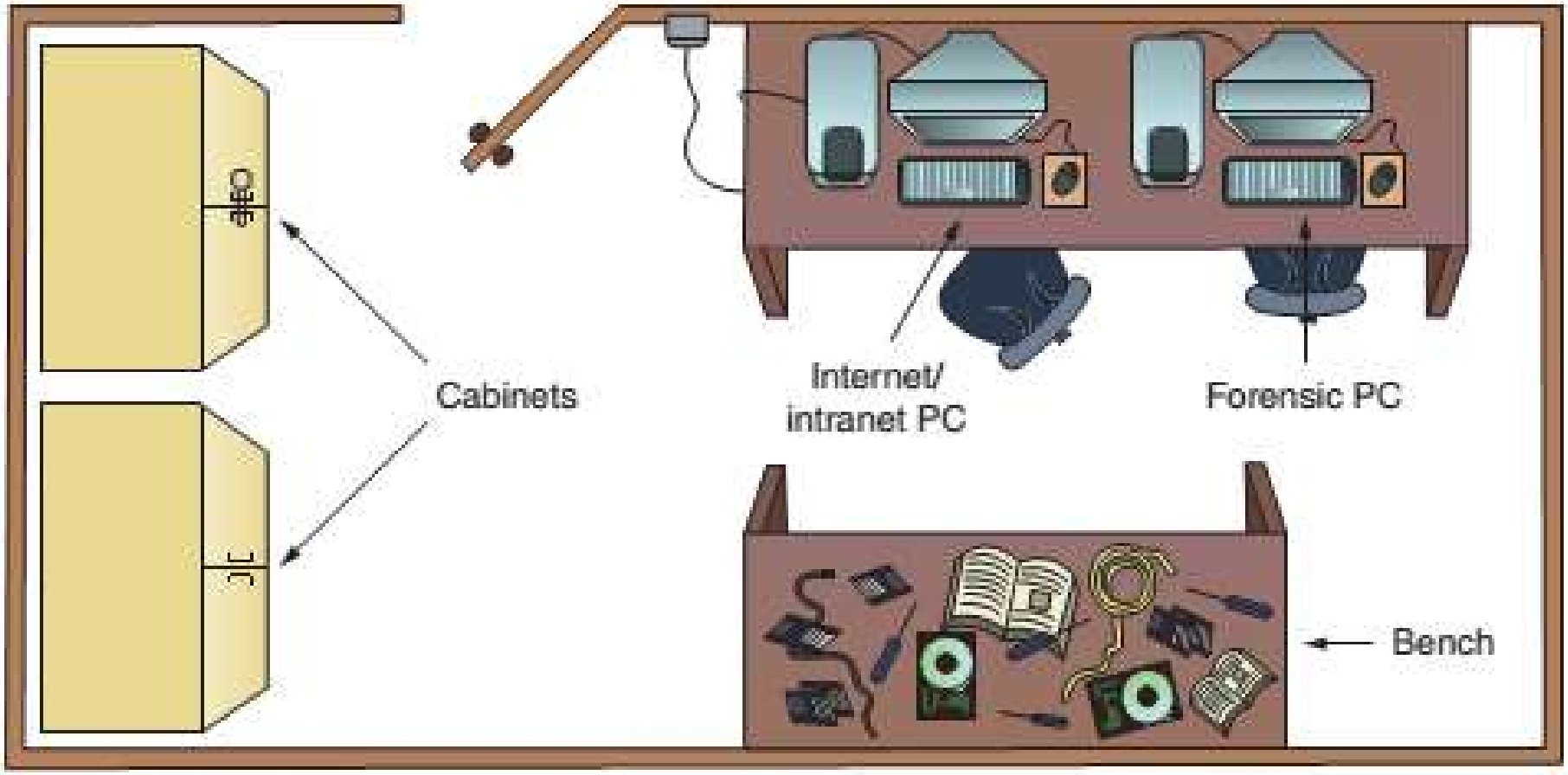
One or two forensic workstations

A research computer with Internet access

*A workbench (if space allows_*

Storage cabinets

Small or Home-Based Lab

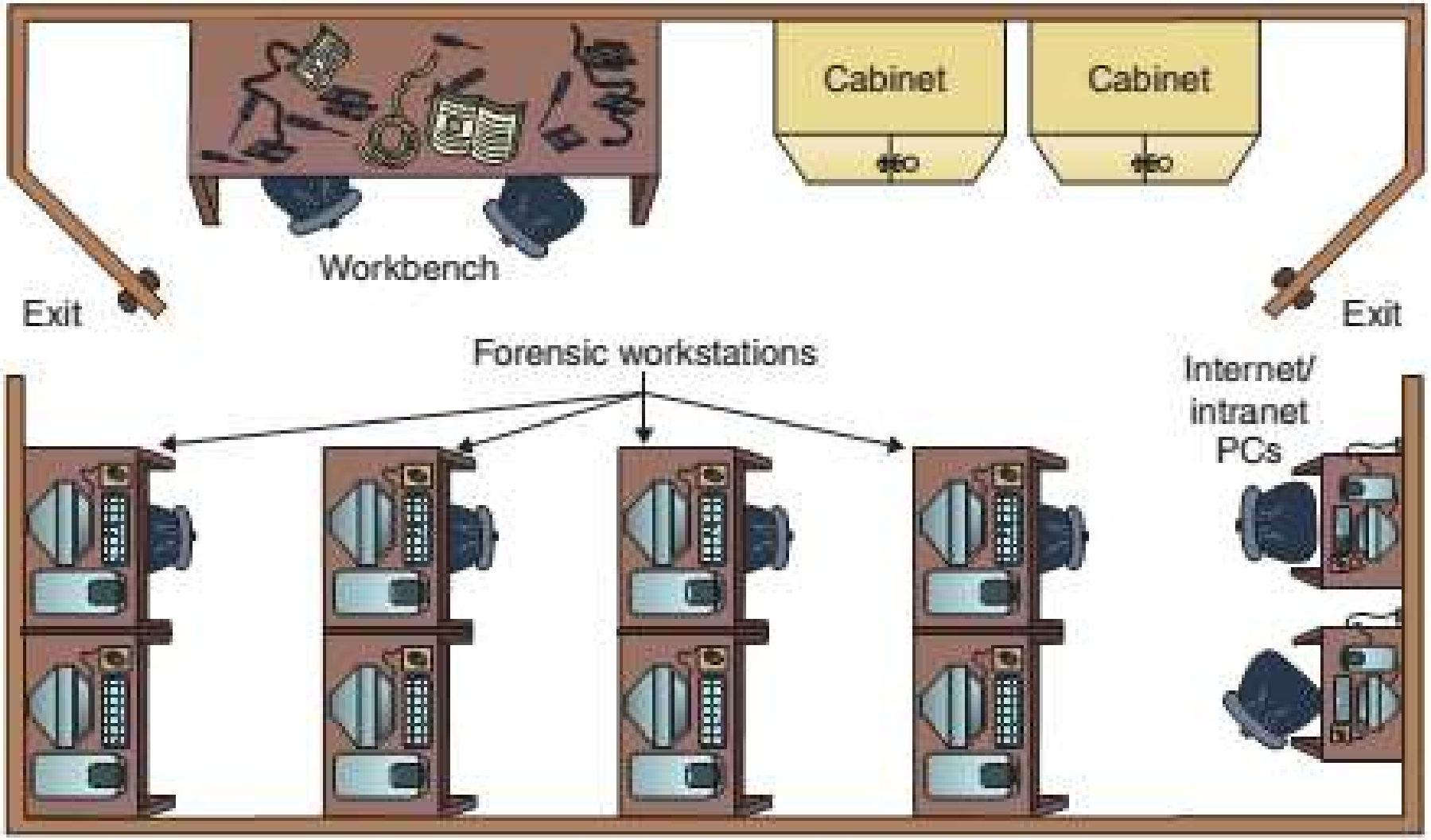


Mid-Size Lab

Mid-size labs are typically those in a private business

- *Have more workstations*
- *Should have at least two exits, for safety reasons*
- *Cubicles or separate offices should be part of the layout to reinforce need-to-know policy*
- *More library space for software and hardware storage*

Mid-Size Lab

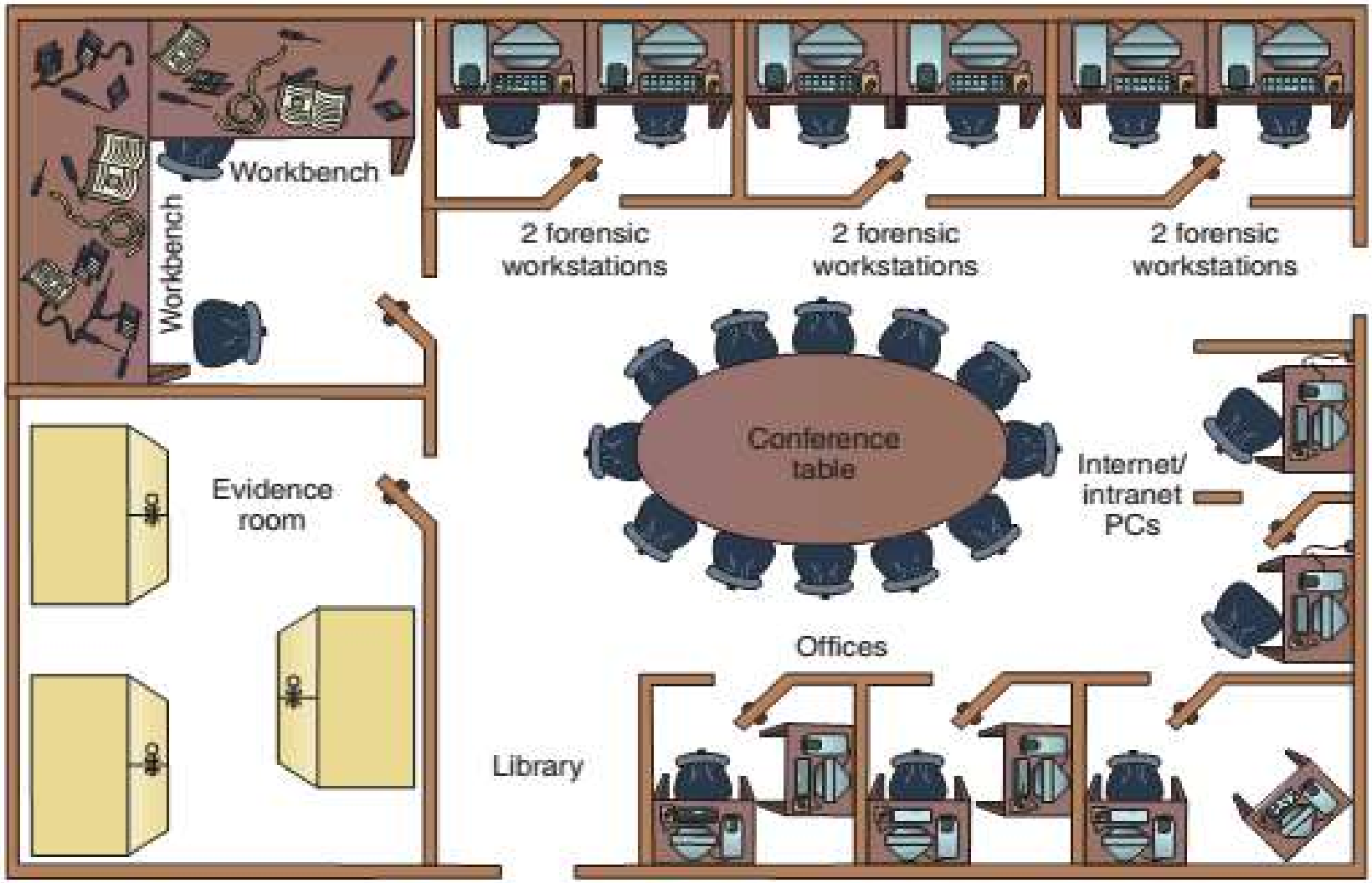


Large or Regional Lab

State law enforcements or the FBI usually runs most large or regional digital forensics labs

- *Have a separate evidence room*
- *One or more custodians might be assigned to manage and control traffic in and out of the evidence room*
- *Should have at least two controlled exits and no windows*

Large or Regional Lab



Forensic Workstation

Selecting a Basic Forensic Workstation

Depends on budget and needs

Use less powerful workstation for mundane tasks

Use multipurpose workstations for resource-heavy analysis tasks

Selecting Workstations for a Lab

Police labs have the most diverse needs for computing investigation tools

A lab might need legacy systems and software to match what's used in the community

A small, local police department might have one multipurpose forensic workstation with one or two basic workstations or high-end laptops

You can now use a laptop PC with USB 3.0 or SATA hard disks to create a lightweight, mobile forensic workstation

Selecting Workstations for Private-Sector Labs

Requirements are easy to determine

Businesses can conduct internal investigations

Identify the environment you deal with

Hardware platform

Operating system

With some digital forensics programs

You can work from a Windows PC and examine both Windows and Macintosh disk drives

Forensic Workstation Hardware

Intel and AMD based PCs

MAC PCs

Linux workstations

Maybe a Sun workstation

Forensic Workstation Storage Hardware

Two or more hard disks per workstation

IDE & EIDE disks (both PATA and SATA)

Fast wide Ultra SCSI card

USB 1.2, 2.0 and 3.0

IEEE 1394 (Firewire)

CD/DVD drive capable of –R, +R, R/W…

Floppy drive

ZIP drive (ZIP100 and 250 and maybe 750)

Forensic Workstation Peripheral Hardware

Any lab should have in stock:

- *Digital camera*
- *Assorted antistatic bags*
- *External CD/DVD drive*
- *IDE cables*
- *Ribbon cables for floppy disks*
- *Extra USB 3.0 or newer cables and SATA cards*
- *SCSI cards, preferably ultrawide*
- *Graphics cards, both PCI and AGP types*
- *Assorted FireWire and USB adapters*
- *Hard disk drives and USB drives*
- *At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter*
- *Computer hand tools*

Forensic Workstation Peripheral Hardware

Write blockers

Prevents writing to the disk

Universal peripheral/disk bridge

Allows an IDE PATA & SATA disks to interface to a computer through a SCSI or USB interface

IDE disk---Bridge---SCSI or USB connector on computer

Often includes write-block capability or used with a hardware write blocker

Forensic Workstation Operating Systems

Windows

NT, 2000, XP, Vista, 7, 8, 8.1, 10

95, 98, ME

Server 2000 thru 2016

MAC

OS X *OS 9* *Maybe earlier versions*

Linux

Red Hat *various versions*

SUSE *various versions*

FreeBSD *various versions*

Ubuntu *various versions*

Kali

…

Forensic Workstation Operating Systems

Maybe a Solaris system

DOS

6.22 *98 (sometimes referred to as DOS 7)*

Maybe copies of other DOSes

DR DOS, PC DOS, …

Be able to prove that all copies of software are legitimate

No pirated copies

Have documented patch histories for all OSs

So, if needed, you can recreate an OS at a particular patch level

Forensic Workstation Operating Systems

Maintain inventory of OSs in original versions

Maintain inventory of all patches, service packs…

Forensic Workstation Application Software

Maintain licensed copies of software such as:

- *Microsoft Office (current and older version)*
- *Hexadecimal editor*
- *Programming languages (Visual Studio, Perl, or Python)*
- *Specialized viewers (Quick View)*
- *Third-party or open-source office suite*
- *Quicken and QuickBooks accounting applications*

Forensic Workstation Forensic Software

At least two GUI forensic software tool sets

e.g., EnCase *(Guidance Software)*

FTK *(AccessData)*

X-Ways Forensics *(X-Ways)*

A Unix/Linux set of software tools

e.g., Cororner's Toolkit, The SleuthKit (TSK), Autopsy

Forensic Workstation Forensic Software

Live CD/USB (both current and past versions)

e.g., *CAINE* *Fedora*

Ubuntu *SLAX*

WHAX *UltimateBootCD*

FIRE (forensic) *Plan-B (forensic)*

Penguin Sleuthkit (forensic)

Backtrack (depreciated)

Kali

Deft

Many others

Forensic Workstation Application Software

Maintain inventories of software application

Include as many versions as possible

Maintain inventories and histories of patches to applications

All applications MUST have licenses

No pirated applications. Courts will throw out the evidence

Keep all applications up to date with patches

But be able go back to an application at a particular patch level if needed

Laboratory Certification

ASCLD

American Society of Crime Laboratory Directors (ASCLD)

www.ascld.org

Sets standards, management, and audit process for labs used in crime analysis including computing-forensics labs

Even those labs used by the police, FBI, and similar organizations

www.ascld-lab.org

Certifies all forensic labs, not just those used for computer forensics

e.g., DNA labs, fingerprint labs, autopsy labs

ASCLD

Nelson writes that

Crime investigations need to be done in an ASCLD-certified lab by a certified forensic specialist

In practice

Crime investigation is often done outside ASCLD-certified labs

ASCLD sets lab requirements such as

Managing the lab

Handling and preserving evidence

Laboratory and investigative procedures

Personnel requirements

Professional development

Reporting

Comments About Lab Certification by ASCLD

ASCLD has set guidelines for digital forensic labs

Forensic labs such as the FBI's Regional Crime Forensic Labs (RCFLs) follow these or similar guidelines

Personal experience of Prof. Lidinsky doing computer forensics:

He did the work using proper procedures including chain of custody and record keeping

*He did **not** do the work in a lab certified by ASCLD*

This fact did not seem to make any difference

Forensic Lab Accreditation

ANSI-ASQ National Accreditation Board (ANAB)

Subsidiary of ANSI and ASQ

Provides accreditation of crime and forensics labs

To be accredited, audits are done on

Lab's tasks and functions

Labs (quality and integrity)

Reference:

www.anab.org/forensics-accreditation/iso-iec-17025-forensic-labs

Business Case for Developing a Forensics Lab

Business Case Comments

Nelson et al seems to belabor the well known and obvious

To me there is nothing new here

Developing a business case for a forensic lab seems similar to developing other business cases

But keep in mind that developing a business case for most things is not always easy

If you find that you need to do a business case

Read that part of the forensics book

Read several of the many other books on doing business cases

Uniform Crime Reports (UCR)

UCR Overview

U.S. crime statistics are reported and categorized in a standard way

Started in 1930

Recommended by International Association of Chiefs of Police

FBI receives the data from many local law enforcement agencies

FBI generates a semiannual UCR based upon this info

Today the UCR is based upon data provided by about 18,000 law enforcement agencies

All crime; not just high tech

UCR Overview

Data is reported in a specific way

By location, specific crime classifications

Specific ways to characterize each crime category in terms of the nature of the crime

FBI provides a handbook telling agencies how and what to report

I have found it difficult to search for specific data in UCR reports

The FBI now offers a tool called *Crime Data Explorer*

Similar interface as census data

UCR Overview

One aspect of the UCR is information on computer crimes

The following is a sample from UCR data used in creating the UCR reports

Excerpt from Older UCR Data

			Intel PC Platform				Apple Platform					
	IDE Drive	SCSI Drive	Win9x	WinNT / 2k / XP	MS Other O/S	Linux	OS 9.x & older	OS X	UNIX H/W	Other H/W	Total Systems Examined	Total HDD Examined
Arson	5	3	3	1		1					5	8
Assault—Aggravated	78	5	31		1	14			1		47	83
Assault-Simple	180	3	77	6	1	32	44	2		1	163	183
Bribery	153		153								153	153
Burglary	1746		1487	259							1746	1746
Counterfeiting & Forgery	1390	4	543	331		309	21	186			1390	1394
Destruction, Damage, & Vandalism	976	48	142	45	29	127	325	90	217	1	976	1024
Drug, Narcotic	1939	24	1345	213		158	213	10			1939	1963
Embezzlement	1023		320	549		23	87	41		3	1023	1023
Extortion & Blackmail	77		2	61		10	3	1			77	77
Fraud	2002		638	932	9	173	55	190		5	2002	2002
Gambling	4910	5	1509	2634		136	138	498			4915	4915
Homicide	36		5	11	9	1	3	7			36	36
Kidnapping & Abduction	2		1	1							2	2
Larceny Theft	7342	56	2134	3093	5	935	127	982	1	21	7298	7398
Motor Vehicle Theft	1747		231	1508		5	1	2			1747	1747

Excerpt from Older UCR Data*
(continued)

			Intel PC Platform				Apple Platform					
	IDE Drive	SCSI Drive	Win9x	WinNT / 2k / XP	MS Other O/S	Linux	OS 9.x & older	OS X	UNIX H/W	Other H/W	Total Systems Examined	Total HDD Examined
Child Porn	593	2	98	162		68	105	160	2		595	595
Robbery	33		23	7			2	1			33	33
Sex Offense—Forcible	80		21	45		1	5	8			80	80
Sex Offense—Non-Forcible	900		324	437		6	90	43			900	900
Stolen Property Offenses	2711	10	800	1634	3	169	53	37	1	9	2706	2721
Weapons Violations	203	1	43	89	2	11	28	31			204	204
Totals Per System	28126	161	9930	12018	59	2179	1300	2289	222	40	28037	28287
	21948		HDD FAT/NTFS	22007	27775			HDD Mac O/S X/Linux/ UNIX	2511			

Thoughts About Older UCR Data

Windows vs. all other attacks

# of crimes using Windows = 21948

# of crimes on all OSs = 27775

21948/ 27775 = ~79% of attacks were on Windows systems

What was the % of OSs that run Windows in the U.S?

What types of crimes are most prevalent?

Larceny & theft: *26%*

Gambling: *17%*

What about sex & child porn crimes that get attention?

Sex & Child Porn: *5.7%*

Table from 2016 UCR
p 67 of Nelson

Crime Statistics For 2016	HDD	Windows OS	Linux	OS X & 9	Other H/W	Mobile Devices	Total Systems Examined
Arson	5	3	1	1	0	0	5
Bribery	6	3	0	1	0	0	4
Burglary	6	0	0	0	0	0	0
Child Porn	29	14	2	7	0	23	46
Counterfeit & Forgery	6	6	0	0	0	1	7
Drug Narcotic	20	7	0	3	0	54	64
Embezzlement	9	9	0	1	1	0	11
Extortion & Blackmail	5	3	2	0	0	1	6
Fraud	13	4	0	7	0	41	52
Gambling	10	7	2	0	0	5	14
Homicide	13	5	0	0	0	3	8
Kidnapping & Abduction	0	0	0	0	0	1	1
Larceny Theft	2	1	0	2	0	0	3
Robbery	1	0	0	1	0	0	1
Sex Offense Forcible	6	4	0	0	0	0	4
Sex Offense Non-Forcible	8	8	0	0	0	8	16
Stalking	15	9	0	5	0	28	42
Stolen Property Offenses	1	1	0	0	0	0	1
Weapons Violations	2	2	0	0	0	0	2
Totals	157	86	7	28	1	165	287

Thoughts About 2016 UCR Data

Windows vs. all other attacks

# of crimes using Windows = 86

# of crimes on all OSs = 122

86/ 122 = ~70% of attacks were on Windows systems

What is the % of OSs that run Windows in the U.S?

What types of crimes are most prevalent?

Child Porn:	*18%*
Drug Narcotic:	*13%*
Fraud+Gambling:	*23%*

What about larceny & theft crimes?

Larceny Theft:	*1.3%*

So What's Changed

% Child Porn ↑ # Child Porn ↓

% Larceny Theft ↓

But what's the big elephant in the room?

Cell phones!

Internet Crime Complaint Center (IC^3)

FBI's IC^3 Overview

Originally a joint activity by FBI and NW3C

Now is an FBI operation

Mission Statement

> *To serve as a vehicle to receive, develop and refer criminal complaints regarding the rapidly expanding arena of cybercrime.*

Issues Cybercrime reports

https://www.ic3.gov

IC³ 2012 Report

Overall Statistics

Total complaints received: 289,874

Complaints reporting loss: 114,908

Total Loss: $525,441,110.00

Median dollar loss for those reporting a loss: $600.00

Average dollar loss overall: $1,813.00

Average dollar loss for those reporting loss: $4,573.0

IC³ 2015 - 2019 Reports
Complaints Stastistics

IC³ 2012 Reports
Types of Complaints

Auto

Selling vehicles that criminal doesn't own over Internet

Government Agency Impersonation

Usually via email to start

Intimidation/Extortion

Email or pop-ups allegedly from well know software firm claiming that software is infected with viruses and must be fixed immediately

Real Estate

Scams: Rental, Timeshare, Loan Modification

IC³ 2012 Reports
Types of Complaints

Hit Man

You get an email saying that sender has been hired to kill you unless you do something such as send money or convert to some specific religion

Ransomware *(e.g., Citadel)*

Virus that freezes your computer and states that you

- Violated a law
- Your IP address visited a child porno site
- Go to DoJ web site it gives you and pay a fine
- Only after you pay the fine will your computer be unfrozen

After you pay fine, virus Citadel continues to be a trojan doing online banking and credit card fraud

IC³ 2012 Reports
Types of Complaints

Romance

Love and romance promised

Perp scans and uses chat rooms, dating sites and social media sites

To build trust, victim initially gets small gifts, poetry, claims of common interest or the promise of companionship

Then the perp

- Suddenly has an emergency and needs money OR
- Asks victim to receive packages and reship them out of country OR
- Other activity that is likely to be nefarious

IC³ 2012 Reports
Types of Complaints

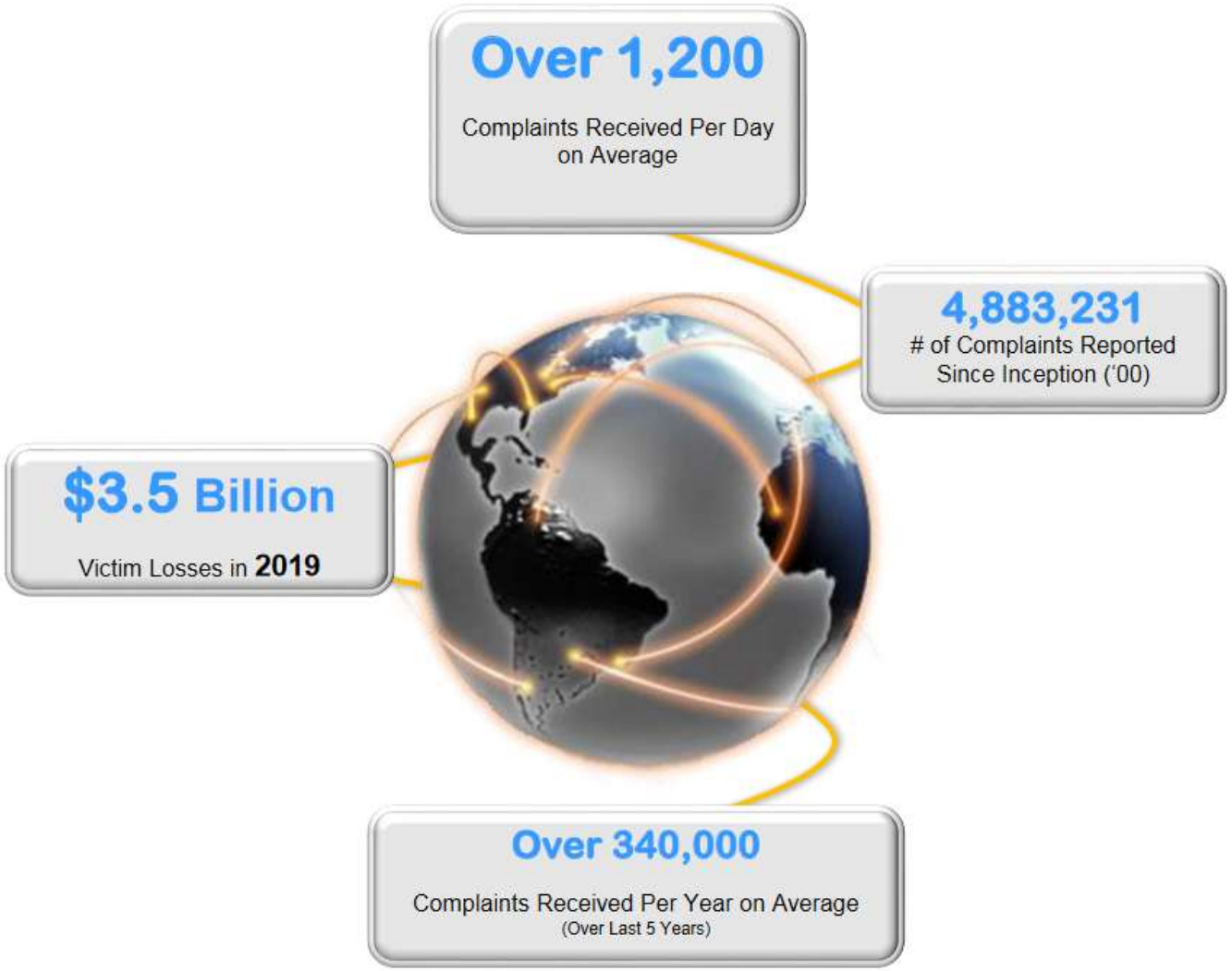
Web sites with

Fake Designer Merchandise

Low Cost versions of expensive software

Ponzi schemes

IC³ 2015 - 2019 Reports
By the Numbers



IC³ 2015 - 2019 Reports
By the Numbers

2019 VICTIMS BY AGE GROUP

Victims		
Age Range[6]	**Total Count**	**Total Loss**
Under 20	10,724	$421,169,232
20 - 29	44,496	$174,673,470
30 - 39	52,820	$332,208,189
40 - 49	51,864	$529,231,267
50 - 59	50,608	$589,624,844
Over 60	68,013	$835,164,766

2019 IC3 Crime Types

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

Descriptors*

Social Media	29,093	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	29,313	

2019 IC3 Crime Types - continued

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

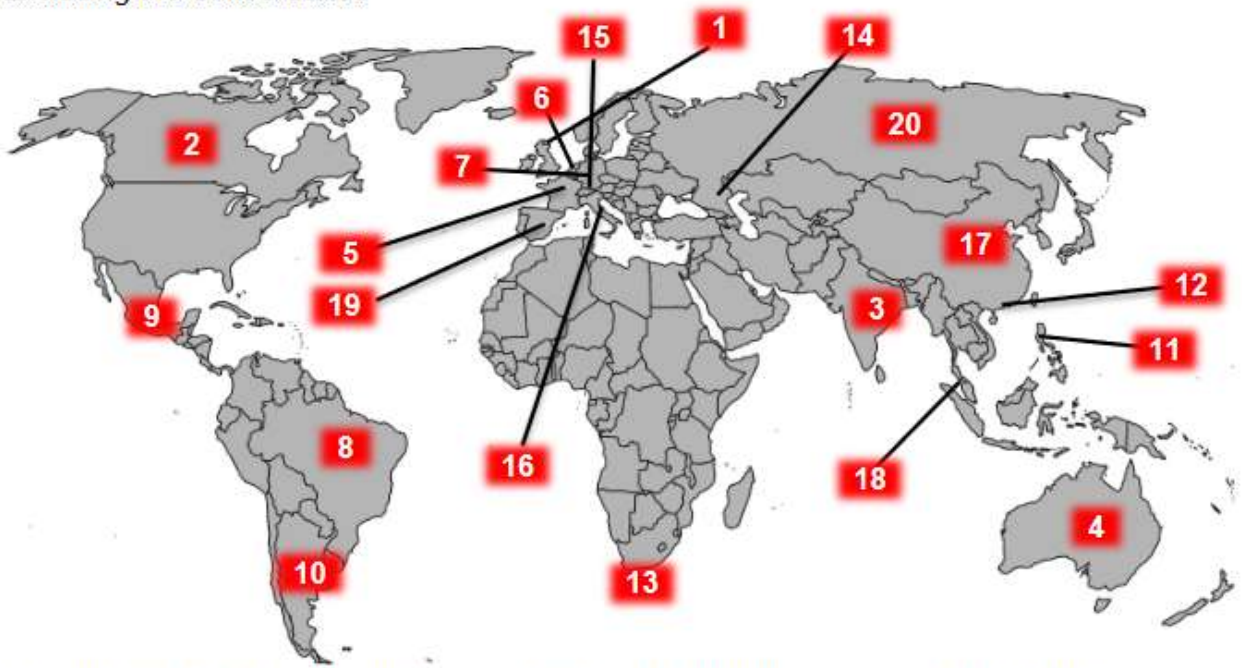
Descriptors*

Social Media	$78,775,408	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	$159,329,101	

IC³ 2019 Reports
Top 20 International Victim Countries

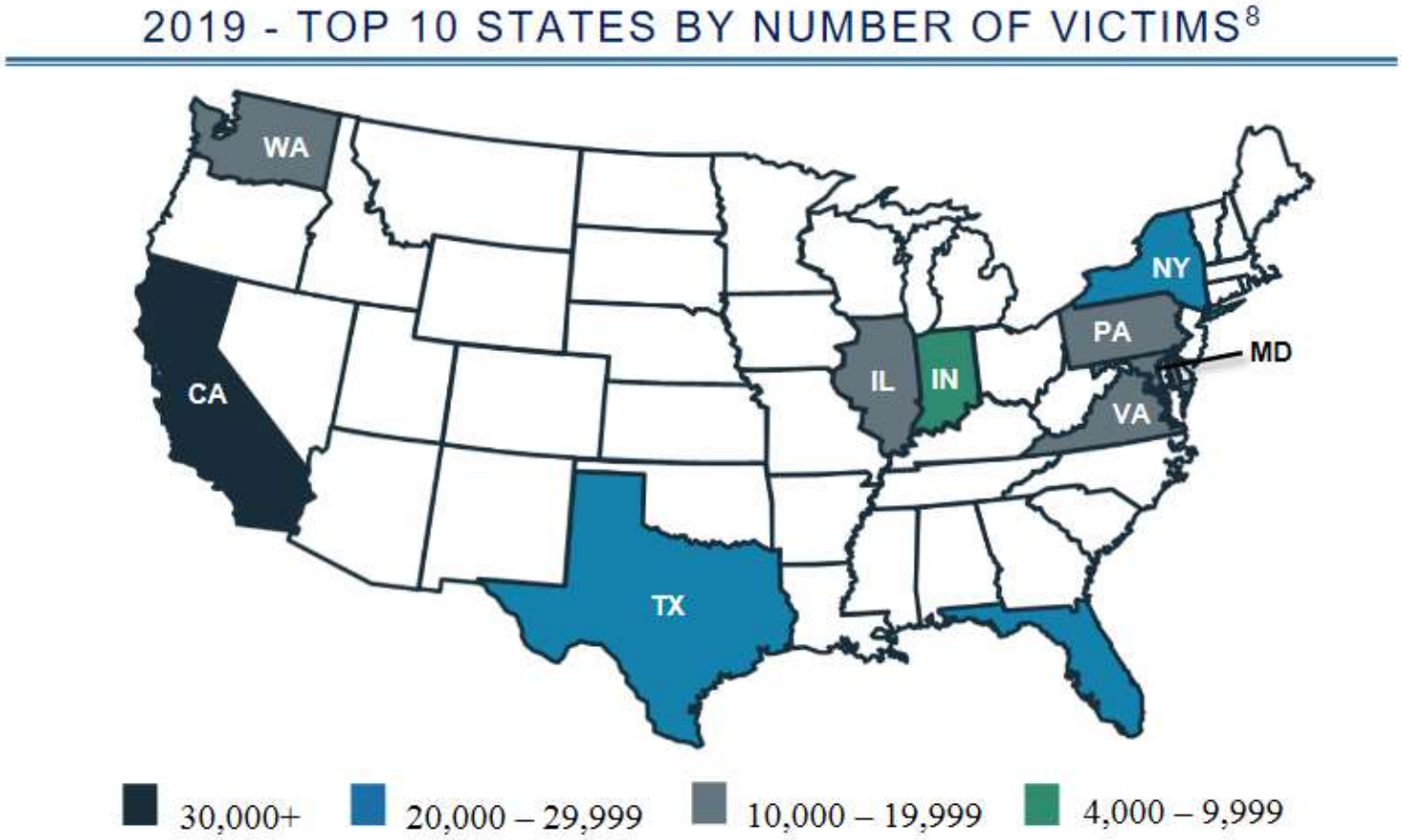
2019 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

Excluding the United States[7]

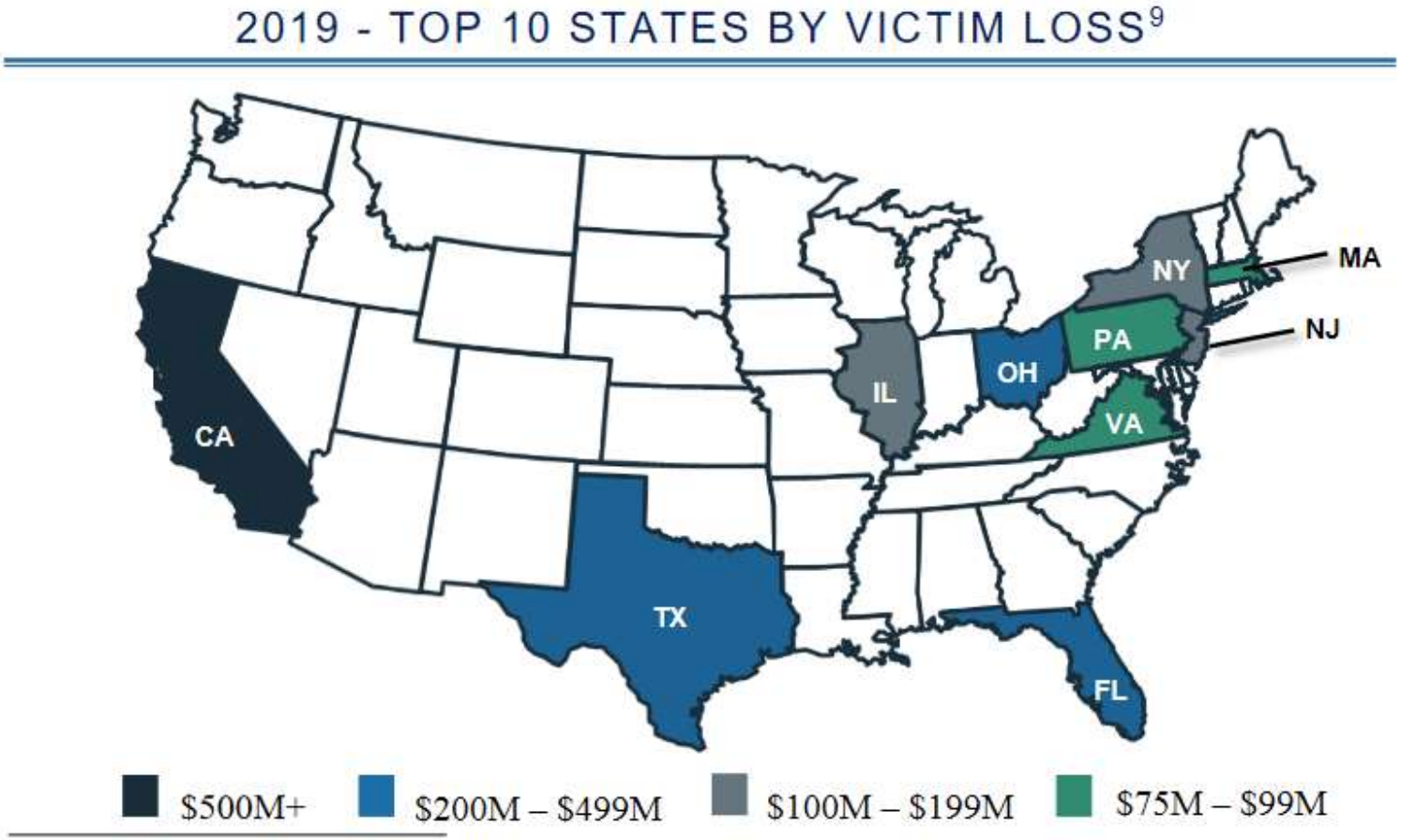


1. United Kingdom	93,796	6. Belgium	1,031	11. Philippines	561	16. Italy	428
2. Canada	3,721	7. Germany	850	12. Hong Kong	535	17. China	403
3. India	2,901	8. Brazil	628	13. South Africa	465	18. Malaysia	362
4. Australia	1,298	9. Mexico	605	14. Georgia	454	19. Spain	358
5. France	1,243	10. Argentina	578	15. Switzerland	438	20. Russian Federation	349

IC³ 2019 Reports
Top 10 States – by # of victims



IC³ 2019 Reports
Top 10 States – by victim loss



Investigator Certification

This topic discusses a number of organizations that certify computer forensic investigators

Investigator Certification
IACIS

International Association of Computer Investigative Specialists (IACIS)

Early professional computing-forensics organization

Created by law enforcement organizations

Members who pass IACIS certification are called

Certified Forensic Computer Examiners (CFCEs)

Goal: Formalize credentials in computing investigations

www.iacis.com

Investigator Certification
IACIS

Three types of membership

Regular

Associate

Fulltime Student

Investigator Certification
IACIS Regular Membership

Regular Membership open to

- *Present or past law enforcement personnel*
- *Government employee*
- *Current full-time forensic contractor for a gov't agency*

Cannot be a Regular Member otherwise

Full benefits

- *Training*
- *Access to experts*
- *Free annual re-certification & one-on-one peer review*
- *Can vote and hold IACIS organization offices*

Investigator Certification
IACIS Associate Membership

Associate membership open to

- *Computer Forensic Practitioners*
- *Open to anyone who can pass a background check*
- *Same as Regular members, but can't vote or hold organizational offices*

Benefits

- *Similar to Regular membership*

Investigator Certification
IACIS Student Membership

Student membership open to

Full-time Students enrolled in accredited school

Benefits

Similar to Associate membership

Investigator Certification
IACIS Training

Basic Computer Forensic Examiner (BCFE) Course

Covers many of the things that you will get in this course

Two-consecutive-week in-person course

No prerequisite knowledge

Costly, but you get a computer, write blocker, external hard drive and other stuff.

Investigator Certification
IACIS Training

Certified Incident Forensics Response (CFIR)

- *Peer review*
- *Prerequisite: The BCFE Course*
- *Exam (includes both practicum and written)*

Re-certification

- *Must re-certify every three years*
- *Keep up with technology changes*

Investigator Certification
Other IACIS Training

ACF: Applied Computer Forensics
BCFE: Basic Computer Forensic Examiner
CIFR: Cyber Incident Forensic Response
Digital Forensics Using Open Source Tools
Mac I: Best Practices in Mac Forensics
Mac II: Advanced Practices in Mac Forensics
Managing a Digital Forensics Lab
MDF: Mobile Device Forensics
PLA: Preparing for Lab Accreditation
RAM Capture and Analysis
SVR: Surveillance Video Recovery
WFE: Windows Forensic Examiner

Investigator Certification
HTCN Training & Certification

High Tech Crime Network (HTCN)

Provides certification for computer crime investigators and computing-forensics technicians

Has four different certifications

Crime Investigator basic *Crime Investigator advanced*

Forensic Technician basic *Forensic Technician advanced*

Membership not restricted

Low cost student memberships available

www.htcn.org

Investigator Certification
HTCN Training & Certification

Certified Computer Crime Investigator, Basic

3 years of law-enforcement or corporate investigative experience

40 hours of training from approved agency, organization or training company

10 or more documented cases in which candidate participated

Certified Computer Crime Investigator, Advanced

5 years of investigative experience in any area

80 hours of related training from an approved source

Must have served as lead investigator in at least 20 cases and were involved with at least 40 cases as a lead investigator, supervisor, or in a supportive capacity.

Total case involvement must be 60 or more

Investigator Certification
HTCN Training & Certification

Certified Computer Forensic Technician Basic

Same requirements for Certified Computer Crime Investigator Basic, but all experience must be related to computer forensics

Certified Computer Forensic Technician Advanced

Same requirements for Certified Computer Crime Investigator Advanced, but all experience must be related to computer forensics

Some approved sources of training are on their web site

Investigator Certification
Some Other Training & Certification

Access Data Certified Examiner

Trains on use of **Access Data** *products*

Do not need to take Access Data training, but must demonstrate that you can use it in order to be certified

EnCase Certified Examiner

EnCE: EnCase Certified Examiner

Trains on use of **EnCase** *software*

Do not need to take EnCase training, but must demonstrate that you can use it in order to be certified

Investigator Certification
Some Other Training & Certification

EC-Council

www.eccouncil.org

SysAdmin, Audit, Network, Security Institute (SANS)

digital-forensics.sans.org/certification

Computer Technology Investigators Network (CTIN)

www.ctin.org

High Technology Crime Investigations Assoc. (HTCIA)

www.htcia.org

International Society of Forensic Computer Examiners (ISFCE)

www.isfce.com

Digital Forensics Certification Board (DFCB)

www.dfcb.org/certification.html

Certified Cyber Forensics Professional

www.isc2.org/ccfp/default.aspx

Investigator Certification
Some Other Training & Certification

Federal Law Enforcement Training Center (FLETC)

www.fletc.gov

Now part of Homeland Security

National White Collar Crime Center (NW3C)

www.nw3c.org