Cybersecurity: Hardware, Memory, and Data Protection

Hardware

- When you talk about your system's memory, what exactly does that mean?

Hardware

- When you talk about your system's memory, what exactly does that mean?

- How much memory does your computer have?

Hardware

- When you talk about your system's memory, what exactly does that mean?
- How much memory does your computer have?
- There's a complete hierarchy of memory, from *RAM* to *cache memory*, as well as hard disk drives and/or solid state drives, on your system.
  - RAM > L3 cache > L2 cache > L1 cache > CPU memory

Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).

Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).

- Disk drives are just storage space; we can’t directly work there. Manipulation and use of data can only take place in RAM, so we have to move data there.

Memory

- Every file on your computer lives on your disk drive, be it a hard disk drive (HDD) or a solid-state drive (SSD).

- Disk drives are just storage space; we can’t directly work there. Manipulation and use of data can only take place in RAM, so we have to move data there.

- Memory is basically a huge array of 8-bit wide bytes.
  - 512 MB, 1 GB, 2 GB, 4 GB…

Memory

Data Type	Size (in bytes)
`int`	4
`char`	1
`float`	4
`double`	8
`long`	8

Memory

- Back to this idea of memory as a big array of byte-sized cells.

Memory

- Back to this idea of memory as a big array of byte-sized cells.

- Arrays are useful for storage of information but also for so-called *random access*.

Memory

- Back to this idea of memory as a big array of byte-sized cells.

- Arrays are useful for storage of information but also for so-called *random access*.
  - We can access individual elements of the array by indicating which index location we want.

Memory

- Back to this idea of memory as a big array of byte-sized cells.

- Arrays are useful for storage of information but also for so-called *random access*.
  - We can access individual elements of the array by indicating which index location we want.

- Similarly, each location in memory has an *address*.

Representation of Memory

- If you've ever head the term "32-bit system" or "64-bit system," it's referring to memory.

Representation of Memory

- If you've ever head the term "32-bit system" or "64-bit system," it's referring to memory.

- A 32-bit system processor can understand and process memory addresses up to 32 bits in length.

Representation of Memory

- If you've ever head the term "32-bit system" or "64-bit system," it's referring to memory.

- A 32-bit system processor can understand and process memory addresses up to 32 bits in length.

- With each bit being a 0 (off, no power) or a 1 (on, powered), that means there are 2^{32} possible memory addresses, or about 4 billion.

Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

  00101001 11010110 00101110 01010111

Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

  00101001 11010110 00101110 01010111

- Computer scientists often refer to such values using *hexadecimal notation*.

  0x

Representation of Memory

- Computers (and programmers!) often need a way to refer to specific addresses in memory, whether for random access or merely for reference purposes.

- Rather than specifying an address as 32 bits:

  00101001 11010110 00101110 01010111

- Computer scientists often refer to such values using *hexadecimal notation*.

  0x 29D62E57

```
Breakpoint 1, 0x004005af in main ()
(gdb) i r
eax    0xb7fb9dbc    -1208246852
ecx    0xbffff340    -1073745088
edx    0xbffff364    -1073745052
ebx    0x0           0
esp    0xbffff320    0xbffff320
ebp    0xbffff328    0xbffff328
...
```

Adapted from an image at codewall.co.uk.

```
Breakpoint 1, 0x004005af in main ()
(gdb) i r
eax    0xb7fb9dbc     -1208246852
ecx    0xbffff340     -1073745088
edx    0xbffff364     -1073745052
ebx    0x0            0
esp    0xbffff320     0xbffff320
ebp    0xbffff328     0xbffff328
...
```

Adapted from an image at codewall.co.uk.

```
Breakpoint 1, 0x004005af in main ()
(gdb) i r
eax    0xb7fb9dbc    -1208246852
ecx    0xbffff340    -1073745088
edx    0xbffff364    -1073745052
ebx    0x0           0
esp    0xbffff320    0xbffff320
ebp    0xbffff328    0xbffff328
...
```

Adapted from an image at codewall.co.uk.

Hexadecimal

Decimal	Binary	Hex		Decimal	Binary	Hex
0	0000	0x0		8	1000	0x8
1	0001	0x1		9	1001	0x9
2	0010	0x2		10	1010	0xA (a)
3	0011	0x3		11	1011	0xB (b)
4	0100	0x4		12	1100	0xC (c)
5	0101	0x5		13	1101	0xD (d)
6	0110	0x6		14	1110	0xE (e)
7	0111	0x7		15	1111	0xF (f)

00101010

00101010

0010 1010

00101010

0010 1010

0x2A

100s	10s	1s
1	2	3

10^2	10^1	10^0
1	2	3

16^2	16^1	16^0
0	2	A

16^2	16^1	16^0
0	2	A

$0 \times 16^2 + 2 \times 16^1 + A \times 16^0$

00101010

0010 1010

0x2A

42

How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.

Image source: howstuffworks.com

How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.

- Volatile memory requires *power.*

Image source: howstuffworks.com

How Memory Works

- With the exception of hard disk space, memory on your computer is *volatile*.

- Volatile memory requires *power.*

- After a limited amount of time with no power, the electrical charge dissipates, and "state" is lost.

Image source: howstuffworks.com

How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.

How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.

- This means that data needs to be moved pretty constantly around between different parts of memory, feeding new information to the processor.

How Memory Works

- Processing of information can only happen, as you might expect, in the *processor*. A 32-bit processor can only process 32 bits (4 bytes) of information at a time.

- This means that data needs to be moved pretty constantly around between different parts of memory, feeding new information to the processor.

- Despite being only able to process limited information at a time, most processors today are about 2-3 GHz.

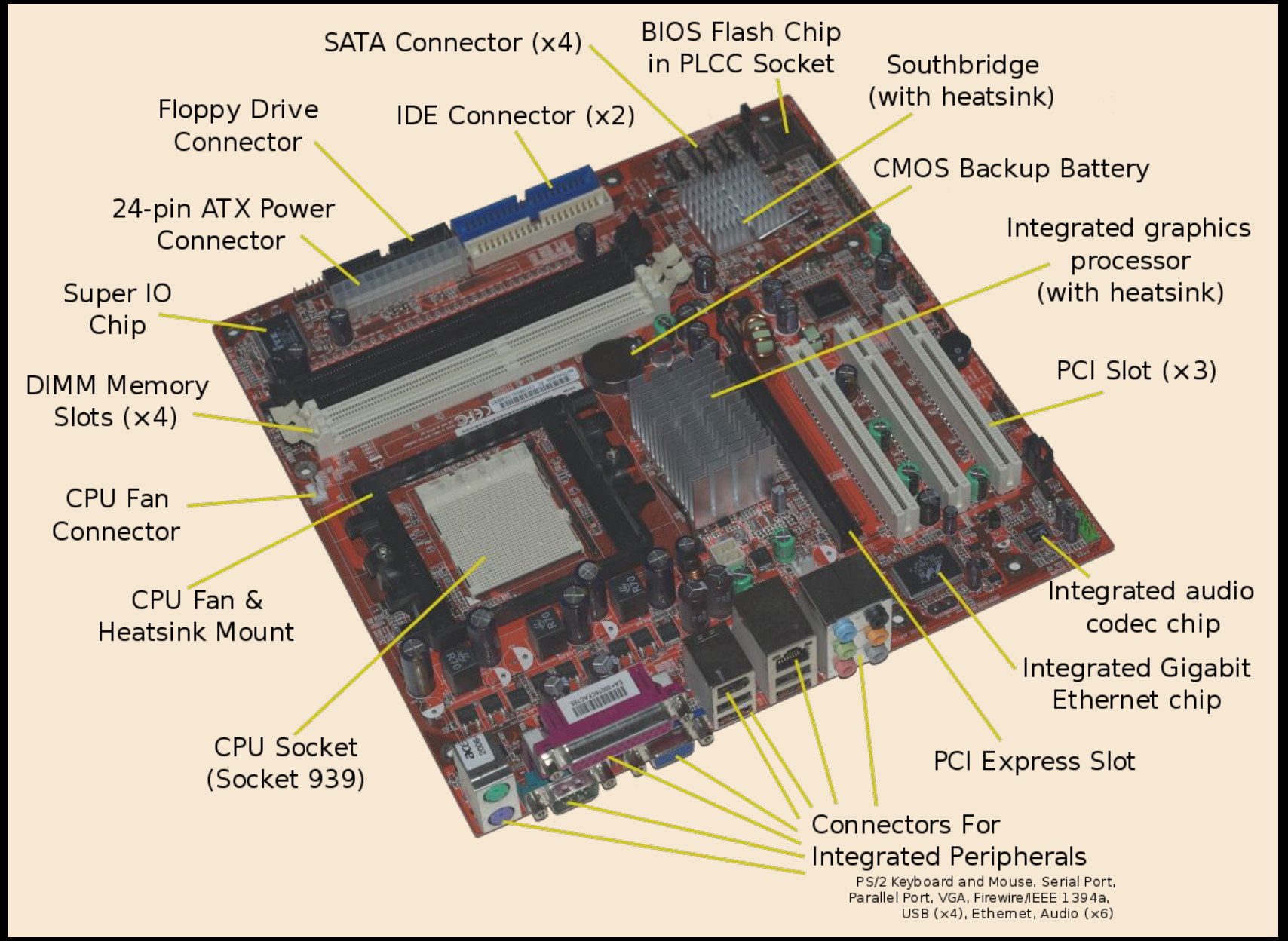

Image source: WikiMedia

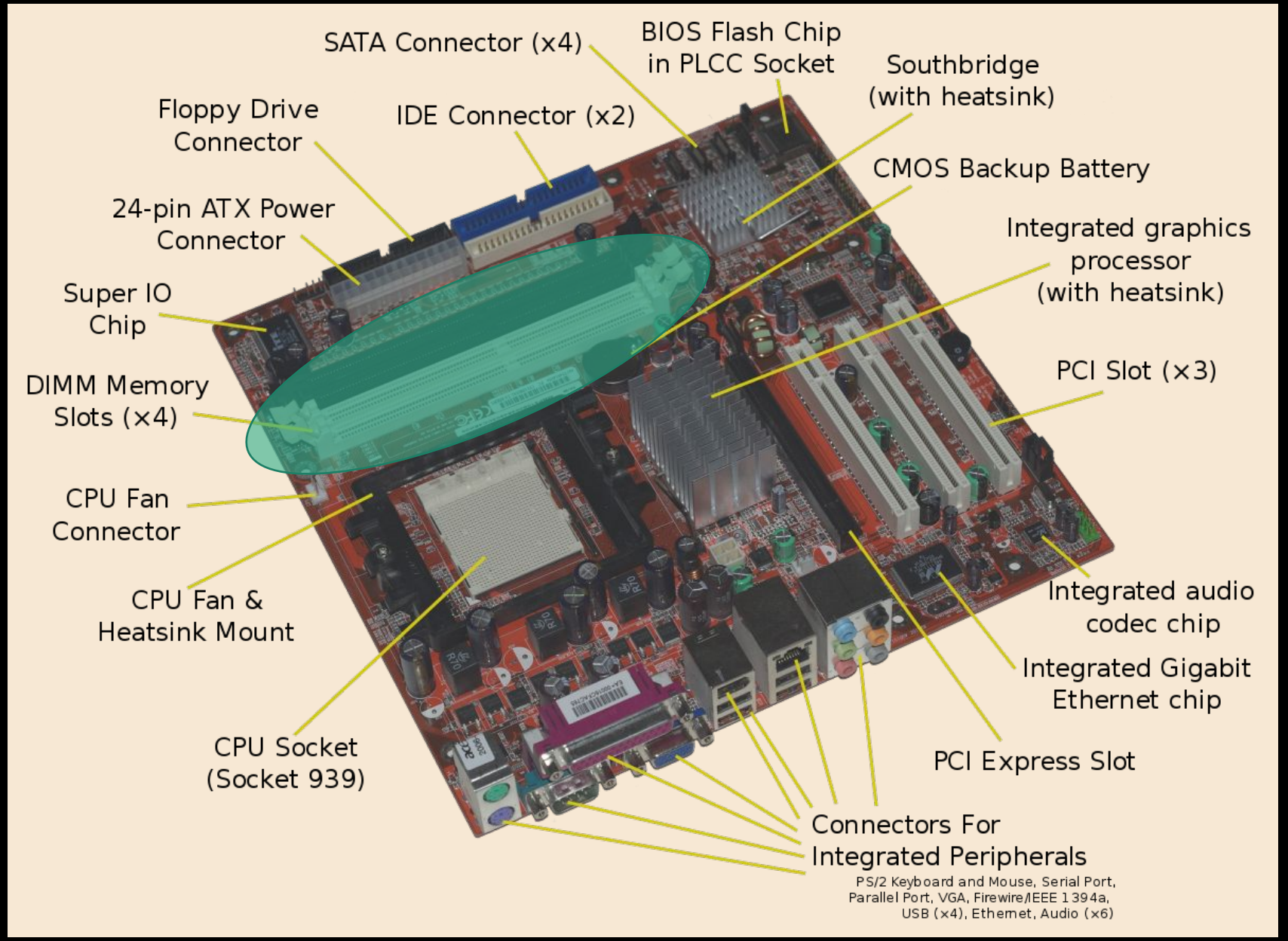

Image source: WikiMedia

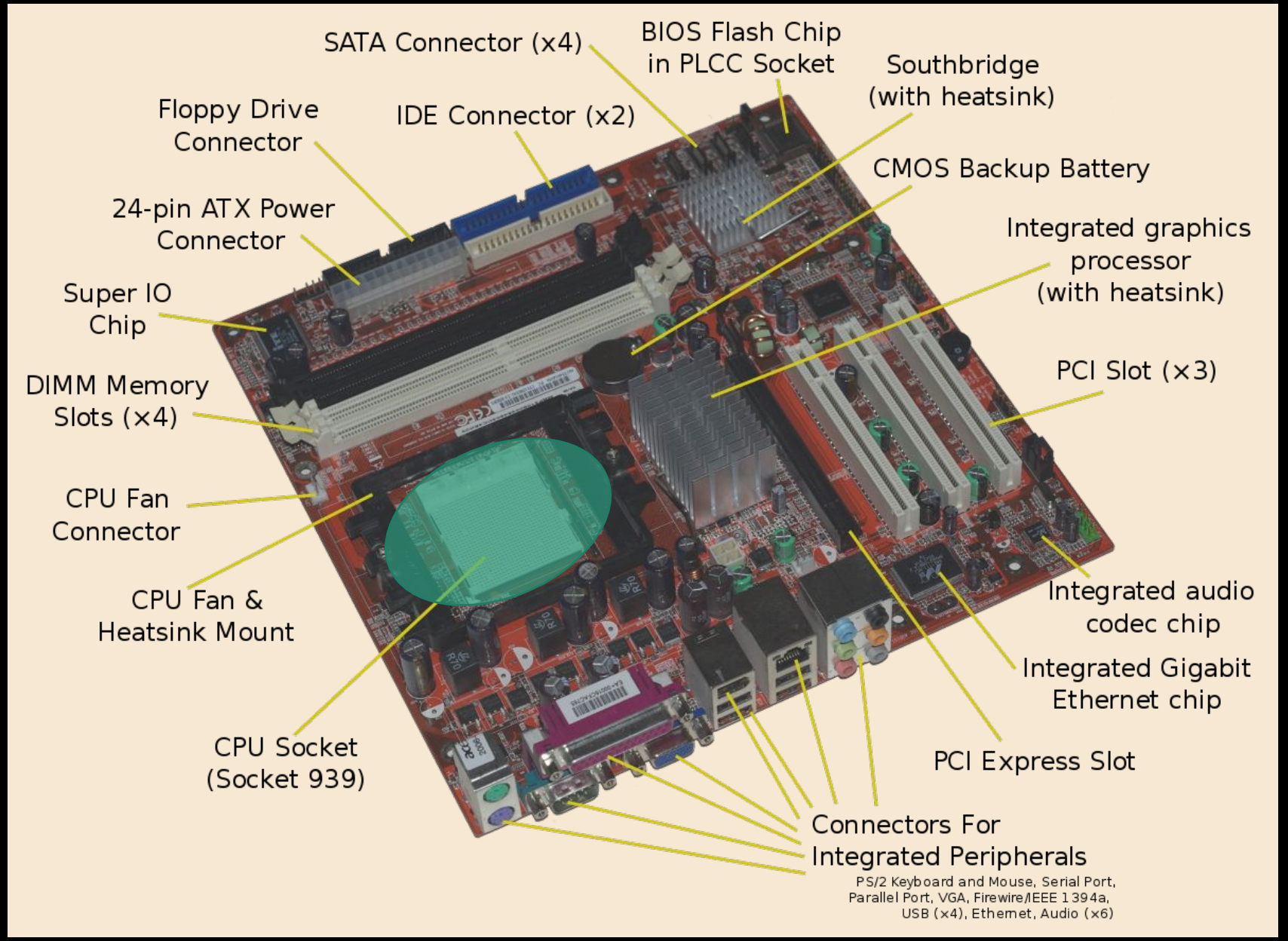

Image source: WikiMedia

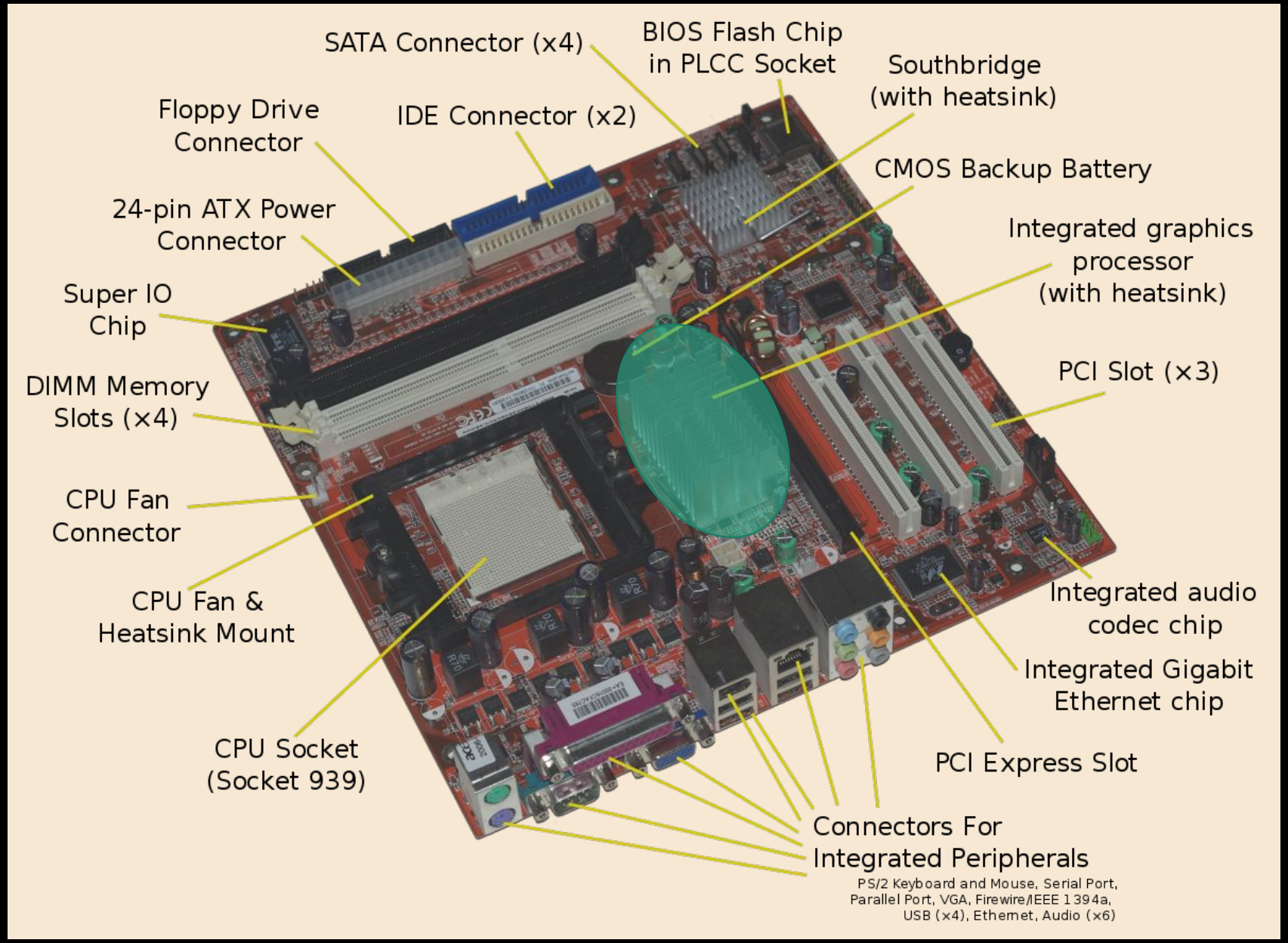

Image source: WikiMedia

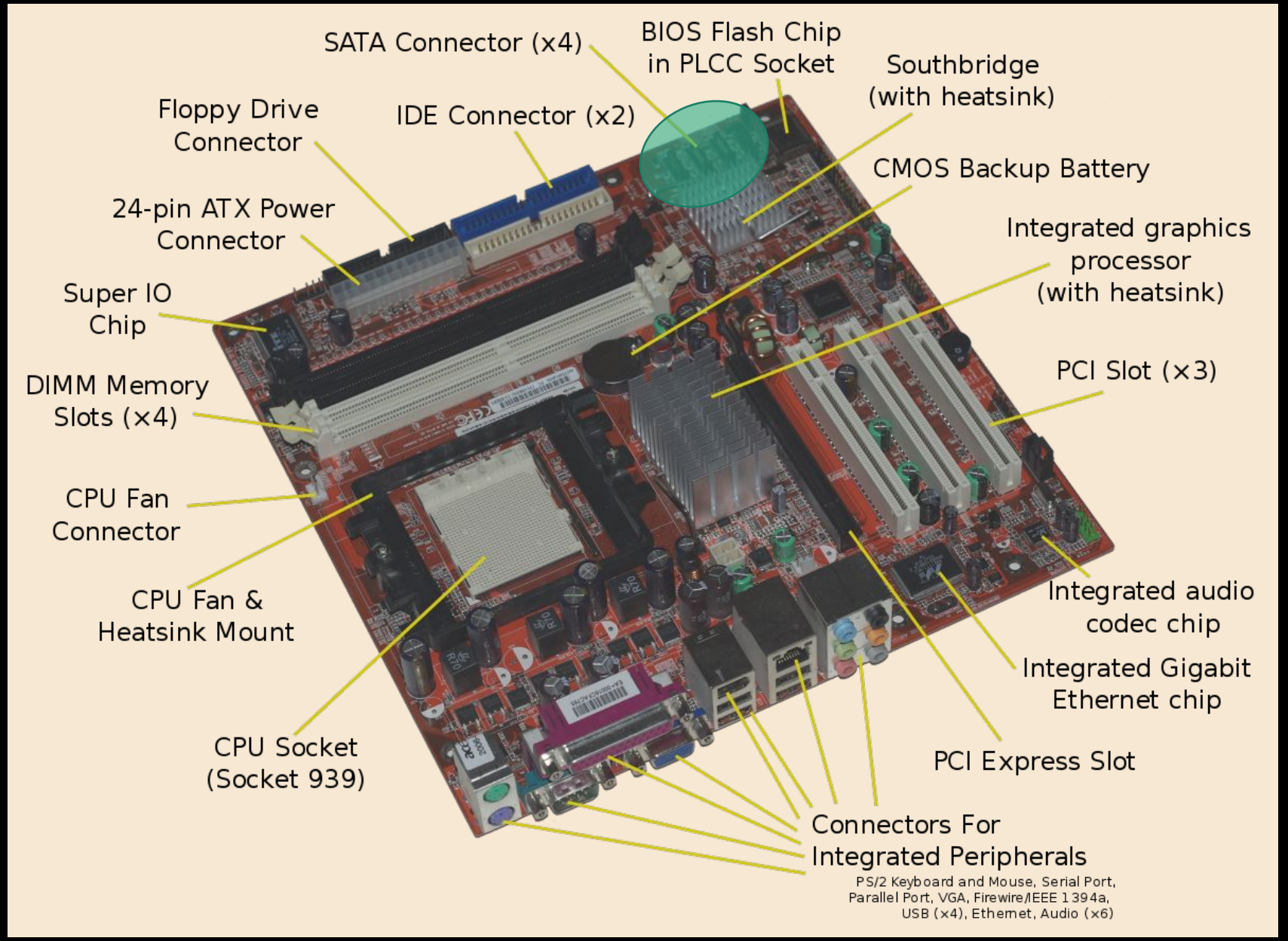

Image source: WikiMedia

How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.

How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.

- Caches (L1, L2, L3) are each successively slower, but each successively cheaper.

How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.
- Caches (L1, L2, L3) are each successively slower, but each successively cheaper.
- RAM is slower, but cheaper.

How Memory Works

- CPU memory is the fastest, least amount of memory on your machine.
- Caches (L1, L2, L3) are each successively slower, but each successively cheaper.
- RAM is slower, but cheaper.
- Hard disk space is pure storage, but insanely cheap.

How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent.*

Image source: geek.com

How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent.*

- It explicitly does *not* require power to work. Rather, each "cell" of memory is written to by way of using magnets.

Image source: geek.com

How Memory Works

- Hard disk space (whether HDD, SSD, or Flash/USB), by contrast, is *non-volatile* or *persistent.*

- It explicitly does *not* require power to work. Rather, each "cell" of memory is written to by way of using magnets.

- Because the magnets do not need power, when the computer shuts off, the data remains.

Image source: geek.com

How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.

How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.

- This is done through a series of connections called *buses* that transfer data from one type of memory to another.

How Memory Works

- As we've seen though, hard disk space cannot be directly manipulated; it has to move to the processor.

- This is done through a series of connections called *buses* that transfer data from one type of memory to another.

- In general, when working on a program, the data for that program (including the code for the program itself) is moved into RAM, and it's manipulated and moved around from there until the program is finished.

Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.

Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.

- Normally, this means that the read/write arm has jammed, or has "bumped" into the spinning platters, which destroys the mechanisms.

Hard Drive Failure

- Because they have literal moving pieces, it's not uncommon for hard drives to fail after a period of time.
- Normally, this means that the read/write arm has jammed, or has "bumped" into the spinning platters, which destroys the mechanisms.
- But a hard drive failure doesn't necessarily mean the data is unrecoverable.

File Deletion

- What happens when we delete files on our machines?

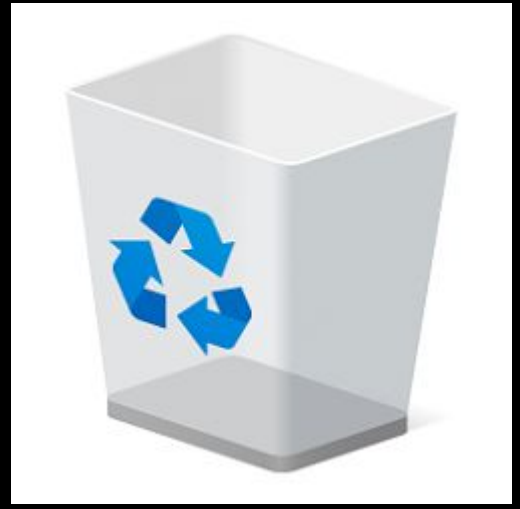

Image source: knowtechie.com

File Deletion

- What happens when we delete files on our machines?

- Overwriting hard disk space is an expensive and time-consuming operation for the machine.

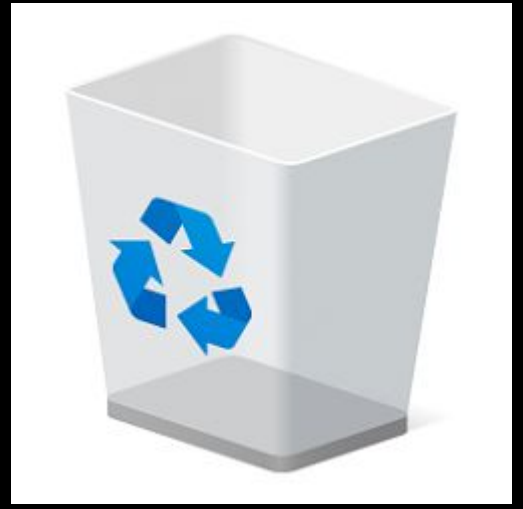

Image source: knowtechie.com

File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.
- Instead, the system just conveniently "forgets" where that data lived, meaning at some point in the future, it may be eventually overwritten.

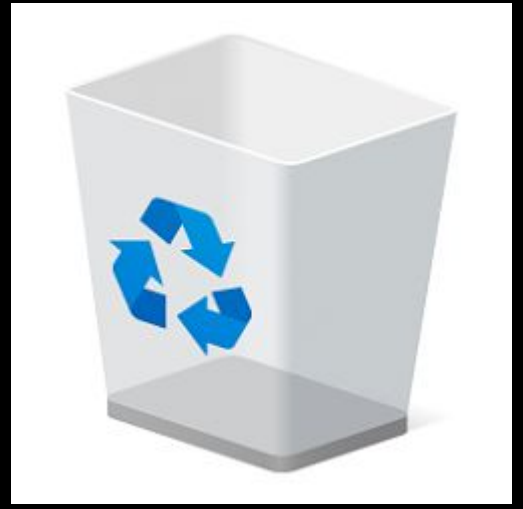

Image source: knowtechie.com

File Deletion

- What happens when we delete files on our machines?
- Overwriting hard disk space is an expensive and time-consuming operation for the machine.
- Instead, the system just conveniently "forgets" where that data lived, meaning at some point in the future, it may be eventually overwritten.

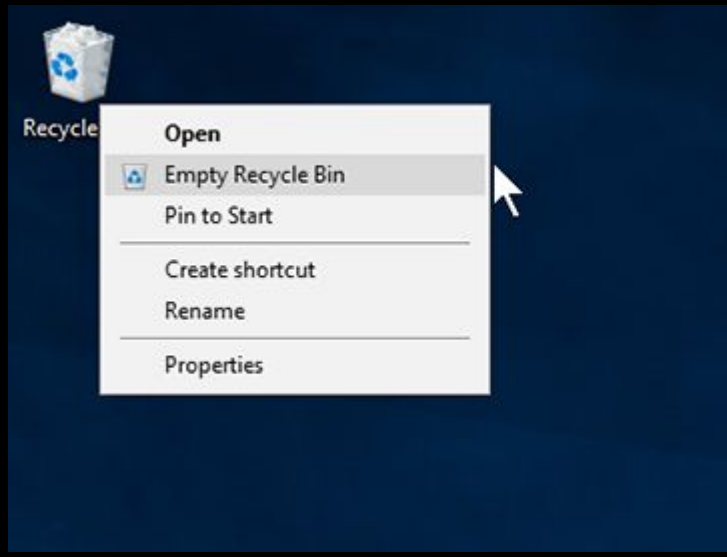

Image source: microsoft.com

Digital Forensics

- So when a hard drive is damaged or files are "deleted," how is it possible to recover information from it?

Digital Forensics

- So when a hard drive is damaged or files are "deleted," how is it possible to recover information from it?

- There are specialized tools out there that can be used to incredibly systematically (and incredibly slowly) read off of "damaged" hard drives bit-by-bit.

Digital Forensics

- So when a hard drive is damaged or files are "deleted," how is it possible to recover information from it?

- There are specialized tools out there that can be used to incredibly systematically (and incredibly slowly) read off of "damaged" hard drives bit-by-bit.

- In both cases, a *forensic image* (essentially, a huge file) that replicates the bit-by-bit content of the hard drive can be created and put onto a functional machine.

Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.

Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.

- Odds are, if this specific sequence appears (it's usually 4-8 bytes), it's the beginning of a file of that type, and it can be read.

Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.

- Odds are, if this specific sequence appears (it's usually 4-8 bytes), it's the beginning of a file of that type, and it can be read.

%PDF

00100101 01010000 01000100 01000110

0x25 0x50 0x44 0x46

Digital Forensics

- Most files have some sort of an identifying "signature" associated with them, also known as a *magic number*.

- Odds are, if this specific sequence appears (it's usually 4-8 bytes), it's the beginning of a file of that type, and it can be read.

%PDF

00100101 01010000 01000100 01000110

0x25 0x50 0x44 0x46

Deleting Files

Image source: dr-fone.com

Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?

Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?

- Physical destruction of the hard drive

Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?

- Physical destruction of the hard drive
- Use a *degausser*

Deleting Files

Image source: dr-fone.com

Deleting Files

- If ordinarily files are not deleted from a hard drive, what can we do to actually really go out of our way to delete data?

- Physical destruction of the hard drive
- Use a *degausser*
- Overwrite with random bits (but not all 0s and not all 1s)

Protecting Client Data

- Odds are, in a large firm environment or as part of an in-house counsel team, this will not all fall to you, but it's very important (and indeed an ABA Model Rule!) to take active steps early on to protect client data.

Protecting Client Data

- Odds are, in a large firm environment or as part of an in-house counsel team, this will not all fall to you, but it's very important (and indeed an ABA Model Rule!) to take active steps early on to protect client data.

- Here are a variety of ways that you as a practitioner can begin instituting best practices for data security.

Protecting Client Data

- Encrypt your hard drive

Protecting Client Data

- Encrypt your hard drive

- Most operating systems provide you with built-in ways to do this now, no reason not to do it!

Protecting Client Data

- Encrypt your hard drive
- Most operating systems provide you with built-in ways to do this now, no reason not to do it!
- Require a password immediately after turning your computer on, before it boots and loads the OS.

Protecting Client Data

- Encrypt your hard drive
- Most operating systems provide you with built-in ways to do this now, no reason not to do it!
- Require a password immediately after turning your computer on, before it boots and loads the OS.
- Some of these systems actually initiate a multi-pass hard drive wipe after *n* incorrect password entries, so don't forget!

Protecting Client Data

- Avoid insecure wireless networks

Protecting Client Data

- Avoid insecure wireless networks

- Though uncommon, unsecured networks provide opportunities for data to be "plucked" out of the air.

Protecting Client Data

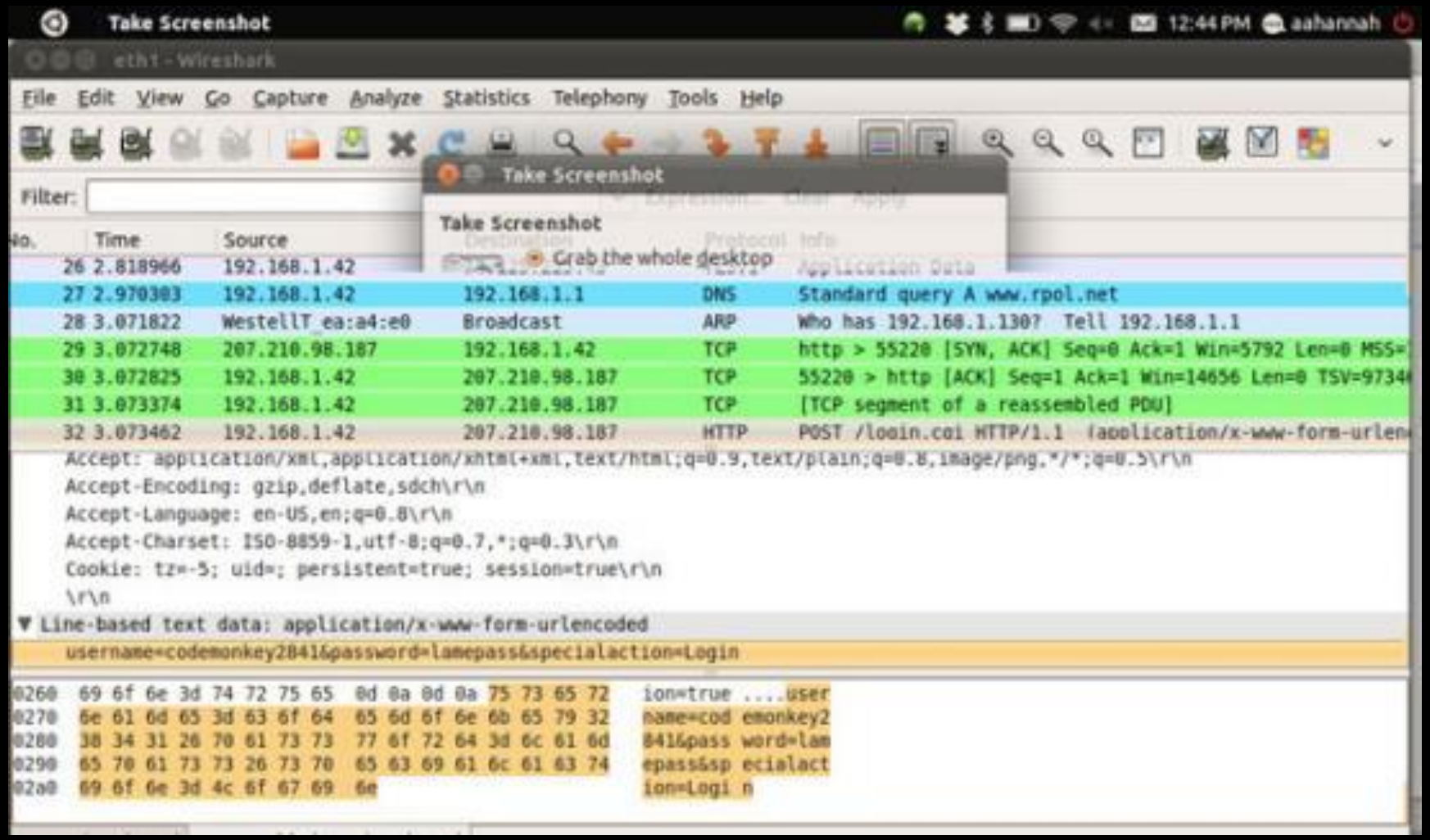

Image source: linuxjournal.com

Protecting Client Data

- Avoid insecure wireless networks

- Though uncommon, unsecured networks provide opportunities for data to be "plucked" out of the air.

- Whenever in an unfamiliar location, rely on private or work-provided VPN services.

Protecting Client Data

- Use password managers

Protecting Client Data

- Use password managers

- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.

Protecting Client Data

- Use password managers

- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.

- Most of these tools also support two-factor authentication.

Protecting Client Data

- Use password managers

- LastPass, 1Password, and others are great services that make it quite easy to more generally secure your access to anything that requires a login.

- Most of these tools also support two-factor authentication.

- Though they sound great, be skeptical. What's one potential problem with tools like this?

Data of 2.4 million Blur password manager users left exposed online

Company says data breach didn't expose any actual passwords stored inside users' Blur accounts.

By Catalin Cimpanu | January 2, 2019 -- 19:51 GMT (11:51 PST) | Topic: Security

Protecting Client Data

- Use complex passwords

Protecting Client Data

- Use complex passwords

- If you would prefer not to use a password manager, at least be certain to use complex passwords.

Protecting Client Data

- Use complex passwords

- If you would prefer not to use a password manager, at least be certain to use complex passwords.

- Passwords with <= 8 characters, you should consider effectively broken already, especially if they only contain letters and numbers.

Protecting Client Data

- Change your passwords

Protecting Client Data

- Change your passwords

- Easier said than done in most cases without a password manager, but rotating through new passwords every 90 days is a good defense.

Protecting Client Data

- Create backups

Protecting Client Data

- Create backups

- Periodically backing up client data preserves your work and their data in the event of a catastrophic hardware failure or "ransom" hack.

Protecting Client Data

- Create backups

- Periodically backing up client data preserves your work and their data in the event of a catastrophic hardware failure or "ransom" hack.

- Back data up to non-network connected machines or to flash drives or disks. (Or to paper files!)

Protecting Client Data

- Have an archival/deletion plan for data

Protecting Client Data

- Have an archival/deletion plan for data

- We tend to think these days that data exists in digital form permanently, but that's not entirely true.

Protecting Client Data

- Have an archival/deletion plan for data

- We tend to think these days that data exists in digital form permanently, but that's not entirely true.

- Develop a consistent plan for deleting and archiving data after a period of time (e.g., 5 years)

Protecting Client Data

- Make talking about data security a priority

Protecting Client Data

- Make talking about data security a priority

- Many people are not as educated about technology as they should be. You don't have to be an expert to have a meaningful discussion about technology in the legal field.

Protecting Client Data

- Make talking about data security a priority

- Many people are not as educated about technology as they should be. You don't have to be an expert to have a meaningful discussion about technology in the legal field.

- Share your knowledge with those around you, and with your clients.

Protecting Client Data

- Establish compliance protocols

Protecting Client Data

- Establish compliance protocols

- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.

Protecting Client Data

- Establish compliance protocols

- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.

- Set regular intervals for "checkups" to ensure this data is protected to the best of your ability.

Protecting Client Data

- Establish compliance protocols

- It's not all that hard to set up most of this stuff early on, it gets a bit harder to do it regularly on top of everything else you do.

- Set regular intervals for "checkups" to ensure this data is protected to the best of your ability.

- Volunteer to work with the compliance team if at a bigger firm.

ABA Formal Opinion No. 477R

May 2017

ABA Formal Opinion No. 483

October 2018

Cybersecurity: Hardware, Memory, and Data Protection