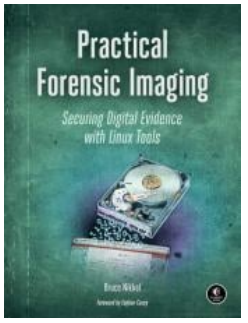
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

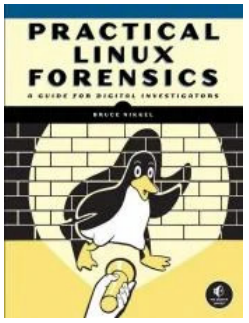
Digital Forensics and Vintage Computing

From Crime to History with New Old Challenges

Prof. Dr. Bruce Nikkel

About me





Career - digital forensics

- 29 years at UBS (retired), 20 years global forensics team
- PhD in digital forensics, author of 2 books on digital forensics
- Elsevier FSI-DI journal (current Editor-in-Chief) 2004-now
- digital forensics professor at BFH 2017-now

Hobby - vintage computing

- vintage computer enthusiast and collector
- volunteer at ENTER computer museum (`www.enter.ch`)
  tour guide, restoration, exhibits, author for HISTEC journal
- teach computer history at BFH 2025-now
- vintage computer forensic projects at BFH 2025-now

Digital Forensics: Who and Why

Crime focused digital forensics

- criminal forensic investigators - Government, Police, Military
- private sector forensics - incident response, e-Discovery, internal and sector-specific investigations
- investigating criminal behavior, IT abuse, employee misconduct, data theft, cyber fraud, espionage, etc.

Discovering an alternate digital forensics community

- 2025 Sabbatical, visited 9 universities with museums
- BFH HKB has a digital forensics lab
- Uni Bern wanted forensic support for a project
- conservators, archives, historians, 'Born Digital' data

I find a growing interest and demand for digital forensics outside the criminal investigation community

Similarities in Digital Forensic Activity

A lot of similarities between crime-focused and history-focused communities

- standard forensic acquisition and analysis processes
- forensic hardware to prevent modification (write-blockers)
- cryptographic integrity preservation (hashes, signatures)
- analyzing filesystems, files, carving unstructured data
- forensic software (FTK, EnCase, Sleuthkit/Autopsy)
- investigative searches for relevant information and documents
- preserving/analysing technical meta data
- reconstructing past events (timelining, super-timelining)
- both provide access to 3rd parties (lawyers or researchers)

Both have passionate and technically skilled people doing the work!

Differences: Crime-focused Forensics

Examples that are different from history-focused digital forensics

- motivation: stop crime, punish the guilty, protect the innocent
- preservation expectation: months or years until court/trial
- evidence can be rejected if proper process not followed
- response times are different, crime needs fast incident response
- hashsets to find known contraband, malware, illegal content
- hardware forensics: extracting evidence from IoT devices
- possible destruction of hardware to gain access to evidence
- high data confidentiality and operational secrecy
- less concern with replicating the operation of original hardware/software (except maybe malware sandboxing)

Exposure to vintage/retro hardware and software is relatively rare

Differences: History-focused Forensics

Examples different from crime-focused digital forensics

- motivation: preserving history, accurate posterity
- preservation expectation: as long as possible (forever)
- might be interesting: fonts/colors used, document layout/structure, organisation of files/folders
- data might be accessed/copied multiple times, over many years, by non-professionals, without protection
- long term storage planning is more important (environmental conditions, bitrot)
- significantly more exposure to vintage/retro hardware and software (also the use of emulators/simulators)

There is probably more, but I am still learning about this focus area

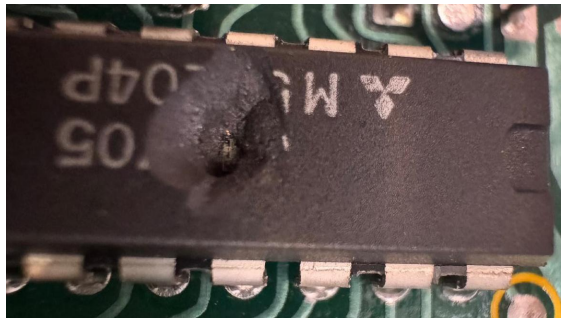
Forensics & Vintage/Retro Computing

I am interested in applying digital forensic tools and techniques to vintage/retro computing

- accessing/recovering data from ancient storage media
- restoration of old hardware into an operational state
- investigation and analysis methods applied to troubleshooting
- malware reverse engineering methods used when there is no technical documentation
- setting up and running old operating systems and applications (on original hardware or emulation)
- provide useable vintage computing environments from historical points in time, for use by 3rd party researchers

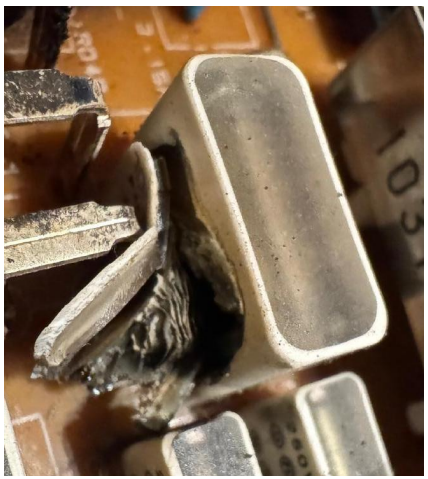
But vintage/retro computing has some challenges...

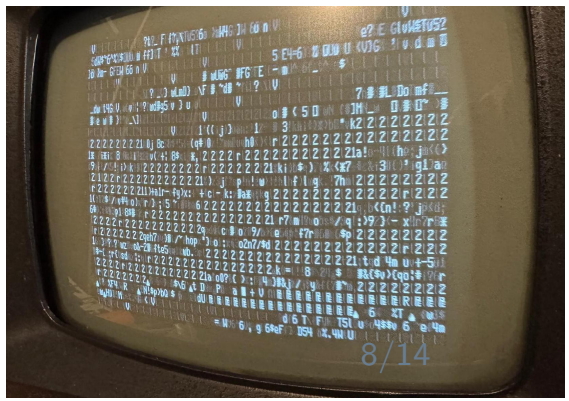
Vintage: Failure/Damage



Old electronics will break/fail

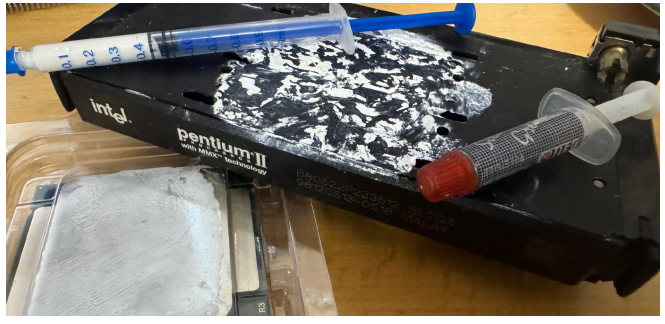
- components leak, fail, or explode (magic smoke)
- chips stuck, dead, or explode
- board corrosion or scratches
- other physical damage (from age or shipping)





Vintage: Risks and Danger

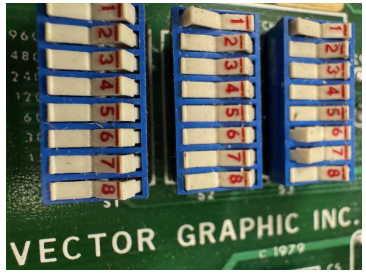
- old dirt and germs
- CRT tubes, high voltage, implosion risk
- high voltage charged capacitors
- high velocity spinning old media
- toxic paste, residue, smoke
- back-breaking heavy! IBM 5120 PC is 45kg

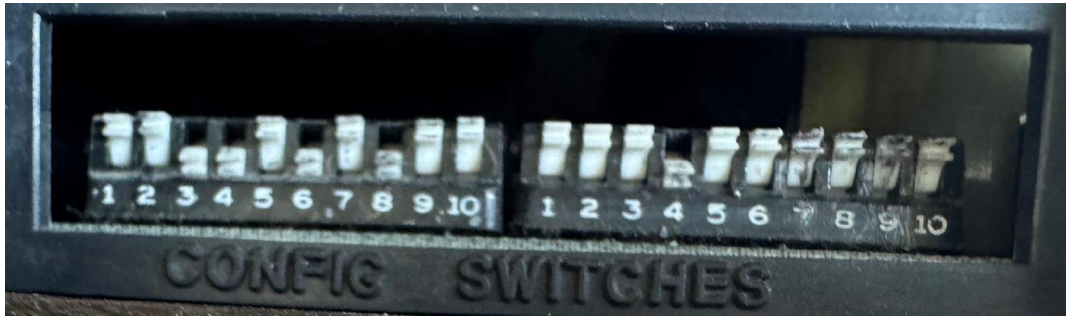


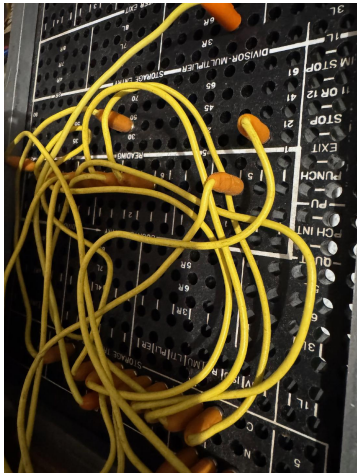
Vintage: Hard Configuration

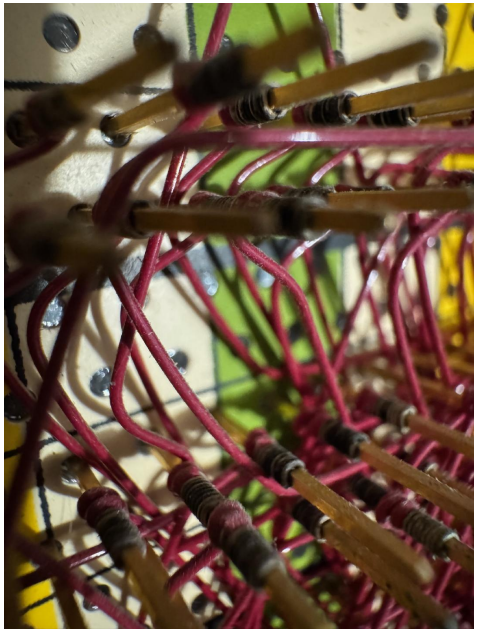
Hardware Configuration/Setup

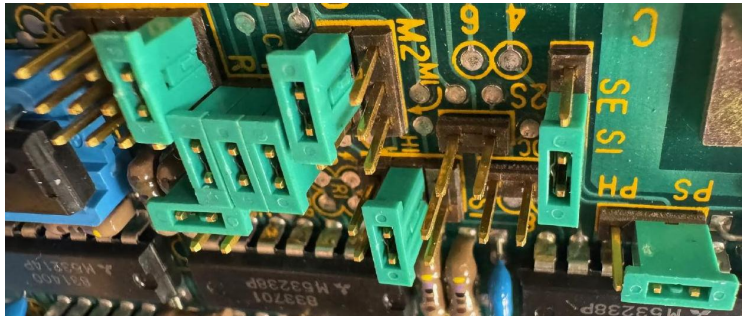
- switches, jumpers
- plugs, wires
- bus termination

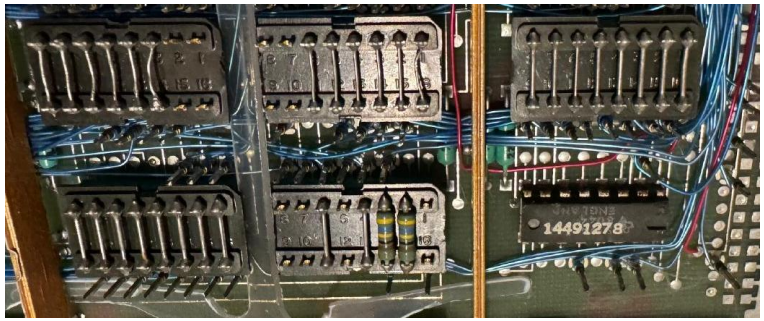






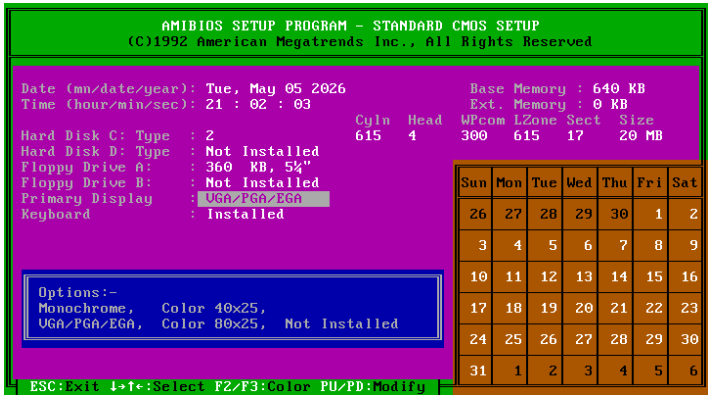


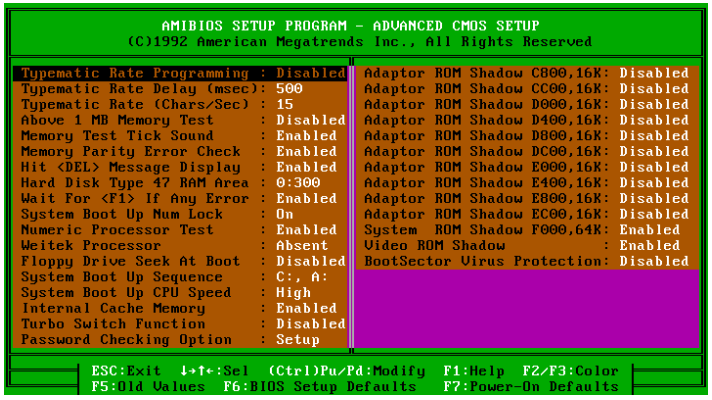


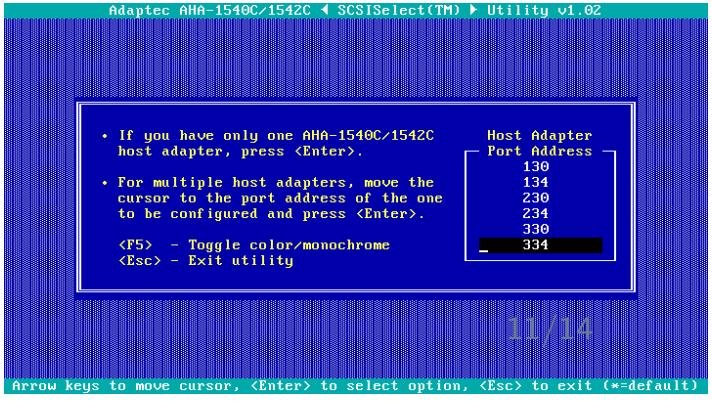


Vintage: Soft Configuration

- mainboard BIOS settings
- expansion card BIOS settings
- OS settings
- Program settings








```
ffmpeg version n8.1 Copyright (c) 2000-2026 the FFmpeg developers
  built with gcc 15.2.1 (GCC) 20260209
  configuration: --prefix=/usr --disable-debug --disable-static --
amf --enable-avisynth --enable-cuda-llvm --enable-lto --enable-fon
nable-gmp --enable-gnutls --enable-gpl --enable-ladspa --enable-lc
e-libass --enable-libbluray --enable-libbs2b --enable-libdav1d --e
dnav --enable-libdvdread --enable-libfreetype --enable-libfribidi
e-libgsm --enable-libharfbuzz --enable-libiec61883 --enable-libjac
libmodplug --enable-libmp3lame --enable-libopencore_amrnb --enable
-libopenjpeg --enable-libopenmpt --enable-libopus --enable-libplac
ble-librav1e --enable-librsvg --enable-librubberband --enable-libs
able-libspeex --enable-libsrt --enable-libssh --enable-libsvtav1 -
libv4l2 --enable-libvidstab --enable-libvmaf --enable-libvorbis --
px --enable-libwebp --enable-libx264 --enable-libx265 --enable-lib
le-libxvid --enable-libzimg --enable-libzmq --enable-nvdec --enabl
nable-opengl --enable-shared --enable-vapoursynth --enable-version
  libavutil      60. 26.100 / 60. 26.100
  libavcodec     62. 28.100 / 62. 28.100
  libavformat    62. 12.100 / 62. 12.100
  libavdevice    62.  3.100 / 62.  3.100
  libavfilter    11. 14.100 / 11. 14.100
  libswscale      9.  5.100 /  9.  5.100
  libswresample   6.  3.100 /  6.  3.100
Universal media converter
usage: ffmpeg [options] [[infile options] -i infile]... {[outfile
```

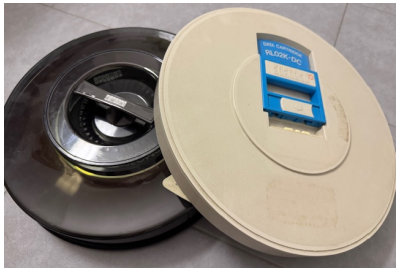
```
[Service]
CapabilityBoundingSet=~CAP_SYS_TIME CAP_WAKE_A
Delegate=
DelegateSubgroup=udev
Type=notify-reload
# Note that udev will reset the value internal
OOMScoreAdjust=-1000
Sockets=systemd-udevd-control.socket systemd-u
Restart=always
RestartSec=0
ExecStart=/usr/lib/systemd/systemd-udevd
FileDescriptorStoreMax=512
FileDescriptorStorePreserve=yes
KillMode=mixed
TasksMax=infinity
PrivateMounts=yes
ProtectHostname=yes
MemoryDenyWriteExecute=yes
RestrictAddressFamilies=AF_UNIX AF_NETLINK AF_
RestrictRealtime=yes
RestrictSUIDSGID=yes
SystemCallFilter=@system-service @module @raw-
SystemCallFilter=~@clock
SystemCallErrorNumber=EPERM
SystemCallArchitectures=native
LockPersonality=yes
IPAddressDeny=any
WatchdogSec=3min
/usr/lib/systemd/system/systemd-udevd.service
```

Vintage: Ancient/Obsolete Media

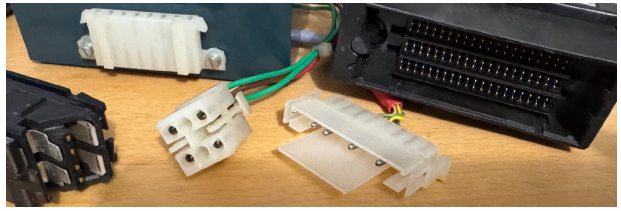
```
$ fls disk.img
Cannot determine file system type
```

```
gpg: public key decryption failed: Operation cancelled
gpg: decryption failed: Operation cancelled
```

- reading obsolete media
- defective drives
- unreadable tapes, floppies
- corrupt filesystems
- partially overwritten data
- missing decryption keys

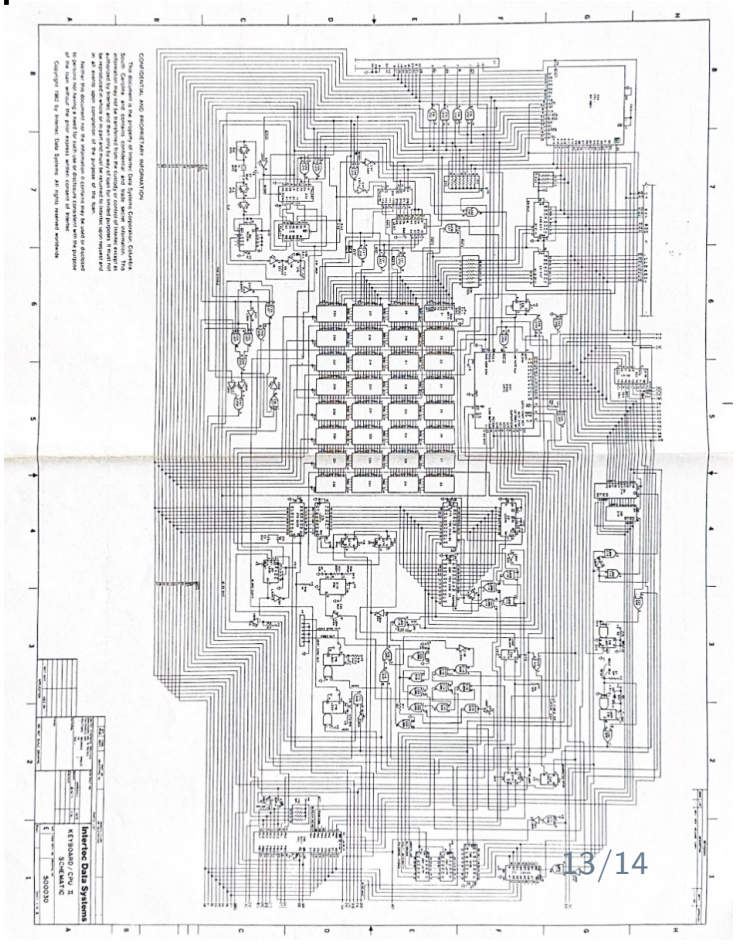


Vintage: Other/Misc



- missing personal knowledge/experience
- missing/bad/complex documentation
- not compatible hardware/software
- missing software, hardware
- missing cables, adapters, drives
- unknown or obscure plugs/cables

```
=== making src ===
make[4]: Entering directory '/home/bjn/devel/HxCFloppyEmulatc
Compiling Fl.cxx...
make[4]: g++: No such file or directory
make[4]: *** [../makeinclude:181: Fl.o] Error 127
make[4]: Leaving directory '/home/bjn/devel/HxCFloppyEmulator
make[3]: *** [Makefile:23: all] Error 1
make[3]: Leaving directory '/home/bjn/devel/HxCFloppyEmulator
make[2]: *** [Makefile:155: ../sources/thirdpartylibs/fltk/fl
make[2]: Leaving directory '/home/bjn/devel/HxCFloppyEmulator
make[1]: *** [Makefile:149: all] Error 2
make[1]: Leaving directory '/home/bjn/devel/HxCFloppyEmulator
make: *** [Makefile:18: HxCFloppyEmulator_software] Error 2
```



Thanks for listening!

Contact me if you...

- have questions or comments
- want to collaborate, do research, or work on projects
- are excited about digital forensics or vintage/retro computing and just want to talk

Prof. Dr. Bruce Nikkel
bruce.nikkel@bfh.ch
Bern University of Applied Sciences
Institute for Cybersecurity & Engineering - bfh.ch/ice
MAS Digital Forensics & Cyber Investigation - bfh.ch/mas-dfci
MSE Information & Cyber Security - bfh.ch/mse
Threema: DC2JN4YK
Mobile: +41 79 255 6316