

TECHNICAL INTELLIGENCE

COMMUNICATIONS

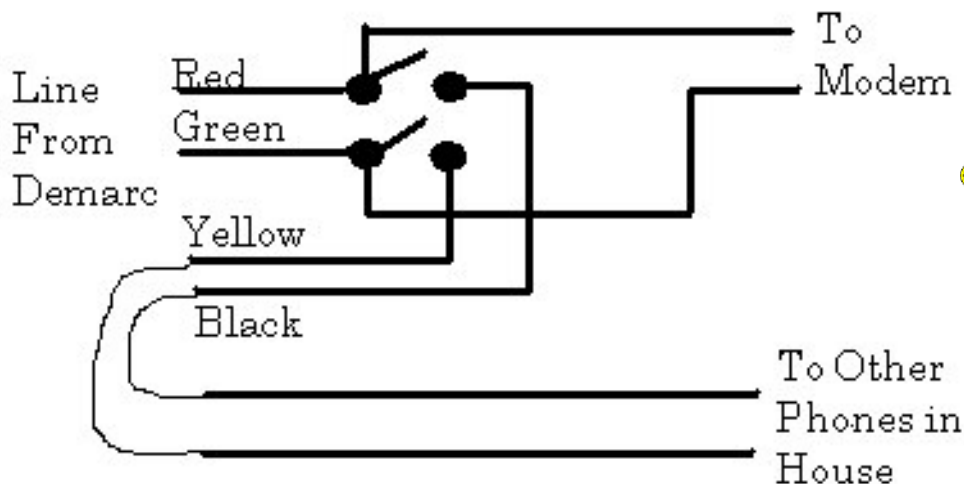


Issue #4, November 2005
<http://www.digivill.net/~ticom/ticomzine/>
email: ticom@digivill.net

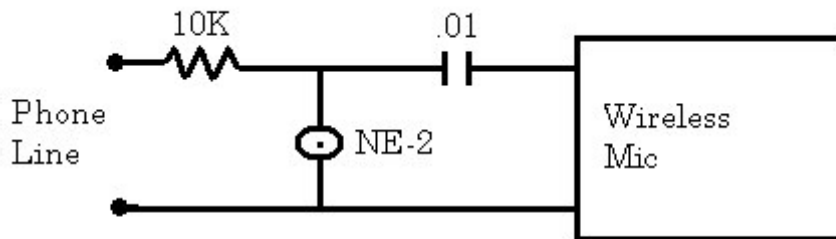
Old-School Phreak Circuits and Data

Over the decades, you collect all sorts of circuits, schematics, and technical data from your explorations, projects, and networking with fellow hobbyists. Here are a couple that are from the early pages in my hack book, and that I have found to be especially useful throughout the years.

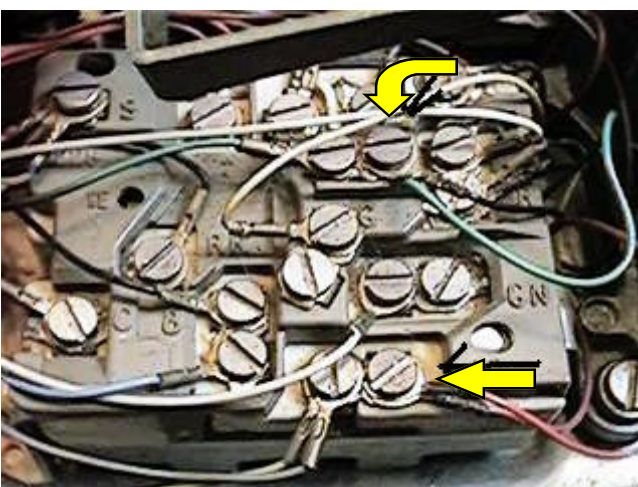
I found this first circuit in the mid-1980s while perusing through a Commodore computer magazine. Back in those days everything was dial-up, and most of us only had a single line in the family household. The switch is a double-pole single-throw toggle switch. What you are doing is routing the phone line from the demarc up to your computer room, and then back down again through the normally unused second pair back to the demarc. You then attach all the other extensions to the yellow and black pair. By doing this you can disconnect all the other phones in the house with a flip of the switch, keep your modem connection from being disrupted, and keep all the other family members from being woken up when you get those 2AM phone calls from other fellow hobbyists.



How to keep a picked-up extension in your house from disrupting a modem connection, and how to keep other phones in house from ringing during late-night H/P sessions.



When I first became involved in the hobby, I discovered a lot of like-minded individuals (LMIs) who didn't own a computer, yet alone a modem. One such person was "H", whom I was introduced to by a mutual hacker friend of ours. "H" was into all sorts of underground arts. We became good friends and started trading information. I received from him a set of about 20 photocopied pages titled simply "Circuits". It was a collection of electronic surveillance circuits that appeared in various underground books and publications during the 1970s. The schematic above was my favorite out of the collection. It replaces the microphone element in a wireless mic, and enables you to attach the device to a phone line. I once put this circuit into a "Mr. Microphone", and used it with a Walkman as a pseudo cordless phone (back when cordless phones were an expensive novelty) so I wasn't tied to a phone during a long conference call.



I am very fond of old Western Electric/Bell System 2500 Touch-Tone desk phones, and I'll snap one up if I find it at a tag sale or flea market although they are becoming harder to find. The one that sits in my computer room I bought for \$5 at a tag sale back in the late 1980s. It was made in 1977, and has outlasted other phones I have acquired since then. The 2500 phones have to be wired properly into the phone pair in order for the touch-tone pad to work. It's simply a matter of reversing the red and green wires on the phone. If you acquire a 2500

phone and the touch-tone pad doesn't work, try that first. The old Bell System phones are phone line-powered and will continue to work in power outages; unlike many of the modern electronic phones that will either not ring, go totally dead, or go off-hook and busy out the phone line when they lose power.

There is a lot of good old-school technical information that is **not** on the Internet, and is waiting to be rediscovered. Where can it be found? At libraries (especially their book sales), used book stores, tag sales, flea markets, and hamfests. On my last trip to have lunch with some friends in upstate New York, I visited a favorite bookstore of mine. Browsing the technical section I discovered a copy of **The Electronic Invasion** by Robert M. Brown, "A completely detailed technical exposure of electronic bugging and de-bugging" circa 1967. Turn off the computer. Go outside into the real world and explore things. Don't be lame.

Hardware Hacking & Reverse Engineering

Dremel Tools & AVI Transponders

Before I was asked to work on my first AVI/ETTM article for another magazine that will remain nameless, the editor of said magazine acquired an AVI transponder tag for experimentation purposes. While doing his weekly radio program, he decided to open the thing up. He used a hammer, and for all intent and purpose demolished the transponder in the process of opening it up. When I examined the device after he had "opened" it, all I saw was a circuit board with snapped-off components. While relating this story to another hacker, he was asked as to why he didn't simply use a Dremel Tool to open it up. His response was "What's a Dremel Tool?"

Dremel is the brand name of a hand held rotary tool made by Robert Bosch Tool Corporation. Their web site is at <http://www.dremel.com/>. With one of these handy little tools you can cut, sand, shape, drill, buff, grind, polish, rout, etch, and clean metal, wood, ceramics, glass, plastic, dry-wall, leather, laminates, and stone. They have models ranging from small battery-powered units to 110V models with flexible shafts and variable speed control. The small battery-operated Minimite model has been a standard piece of equipment for many a hardware hacker. Starting at about \$40 for the Minimite, a Dremel Tool is a must-have for your toolbox. With one of these and a Leatherman Tool, you'd be amazed at what you can do.



Photo from Dremel's web site.

<http://www.dremel.com/>

I recently had the opportunity to examine an AVI transponder that a friend had ordered for his vehicle. While opening this one up was out of the question, there was some useful information on the case. The case contained the FCC ID of the unit, and some patent numbers. Using web sites provided by Uncle Sam, you can find quite a bit of useful information about the device in question. In this instance, I discovered this particular transponder was a "Flat Pack Transponder FPT 2000" made by Mark IV Industries. It operates on 915 MHz. The FCC ID and patent numbers were as follows: FCC ID - JQU801090, Patents - 4870419, 4937581, 5132687, 5164735, 5192954, 5196846. The web sites you can use to look up FCC ID and patent information are: <https://gullfoss2.fcc.gov/prod/oet/cf/eas/reports/GenericSearch.cfm> and <http://www.uspto.gov/patft/index.html> I included some of the information about the FPT2000 that was found on the FCC web site to give you an idea of what you can find. Between these web sites and being properly equipped with the right tools such as a Dremel, you can get your hardware hacking and reverse engineering hobby off to a good start.

The Reader/RF modules are FCC Part 90 compliant and are typically mounted beside the roadway in a cabinet. The RF modules are connected to the antennas by means of co-axial cables. Transponder installation instructions are provided in Attachment A.

In operation, the Reader via a selected RF module sends out a 915 MHz data stream in the format described below to each antenna in turn thereby establishing an intermittent RF field in each lane of the roadway. When a vehicle equipped with a transponder enters the field the pulses activate the transponder and cause it to respond with a data transmission on a carrier frequency of 915 MHz. It should be noted that the transponder is only activated when a 20 microsecond "wake-up" pulse is received. It will not radiate energy at any other time. Transponder radiation will be obscured by the stronger Reader RF field. The Transponder Tx data is received by the antenna which passes it to the RF module for detection and then to the Reader for decoding. If the Reader determines that re-programming of the transponder is necessary, the Reader sends an additional pulse stream to the transponder for that purpose.

When the above process is completed on a given lane, it is repeated in the next lane and so on until as many lanes as necessary up to the full 8 lanes have been scanned. The timing for this process which shows RF activity for one lane is depicted in Figure 2. During a typical passage of a vehicle through a lane the transponder is typically read and programmed twice to confirm accuracy of the data and its CRC.

1.4 Transponder Overview

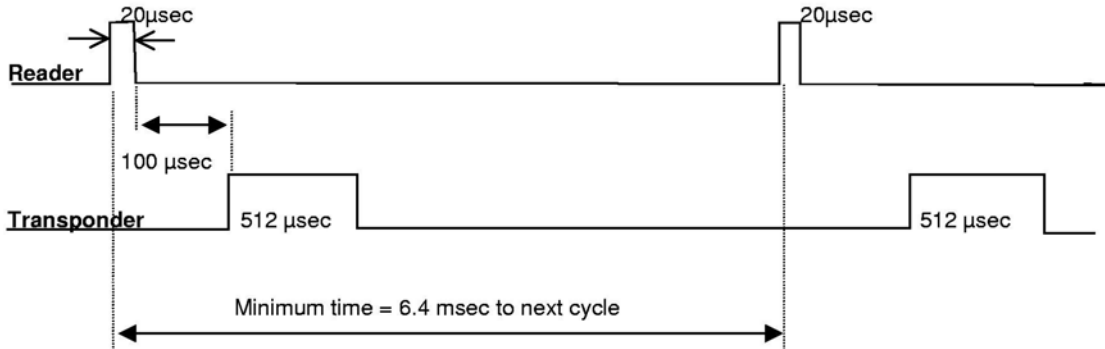
The Transponder consists of two major components: the case and a circuit board. The Transponder transmits and receives Manchester encoded data streams in the 915 MHz frequency band. On-Off Keying modulation is used.

There are five major electronic subsystems on the circuit board:

1. The "hook" Antenna which receives and transmits RF energy
2. The RF Transmitter has two sub-sections. An RF Oscillator that is turned on by the ASIC during the entire time the Transponder transmits. The modulator which converts the baseband Manchester encoded data delivered from the ASIC to the 915 MHz band using OOK (On-Off Keying) data stream.
3. The Receiver which demodulates the 915MHz band RF pulses received from the reader via the antenna.
4. The ASIC which provides: Rx, Tx data and control interfaces, Manchester encoding/decoding, CRC generation/detection. The control interfaces keep the transponder circuitry in low current ("idle mode") until a trigger pulse of between 10 and 30 microseconds is detected. The ASIC transmits a Manchester encoded 256 frame at 500 kilobits per second when a valid trigger pulse is detected. The ASIC only stores the incoming bit stream if the CRC is correct.
5. The Battery which provides 3.60 volt power to operate the transponder.

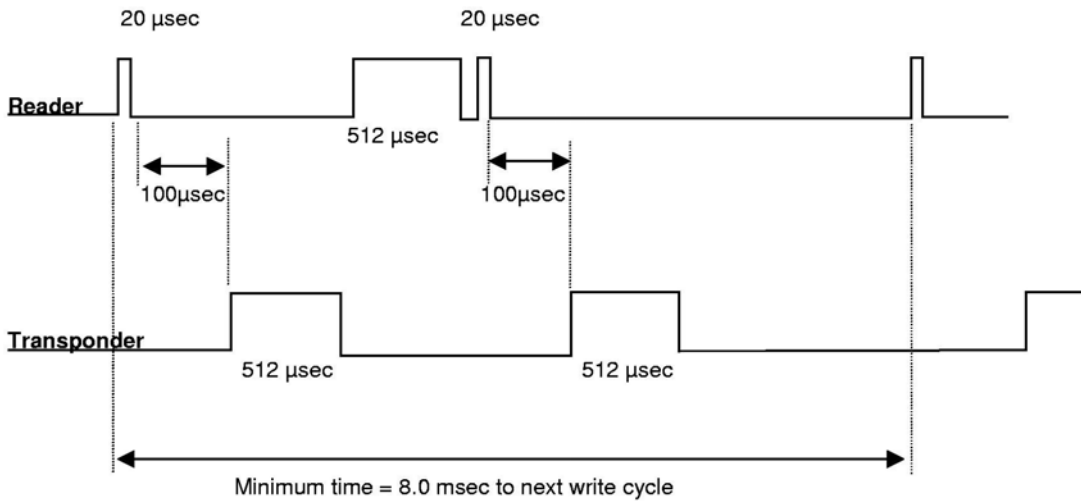
Figure 2 - System Timing Diagram

READ CYCLE



Transponder responds to each trigger pulse by transmitting a 512 microsecond Manchester encoded RF burst (500 kbit/second data rate)

WRITE CYCLE



Transponder responds to each trigger pulse by transmitting a 512 microsecond Manchester encoded RF burst (500 kbit/second data rate)



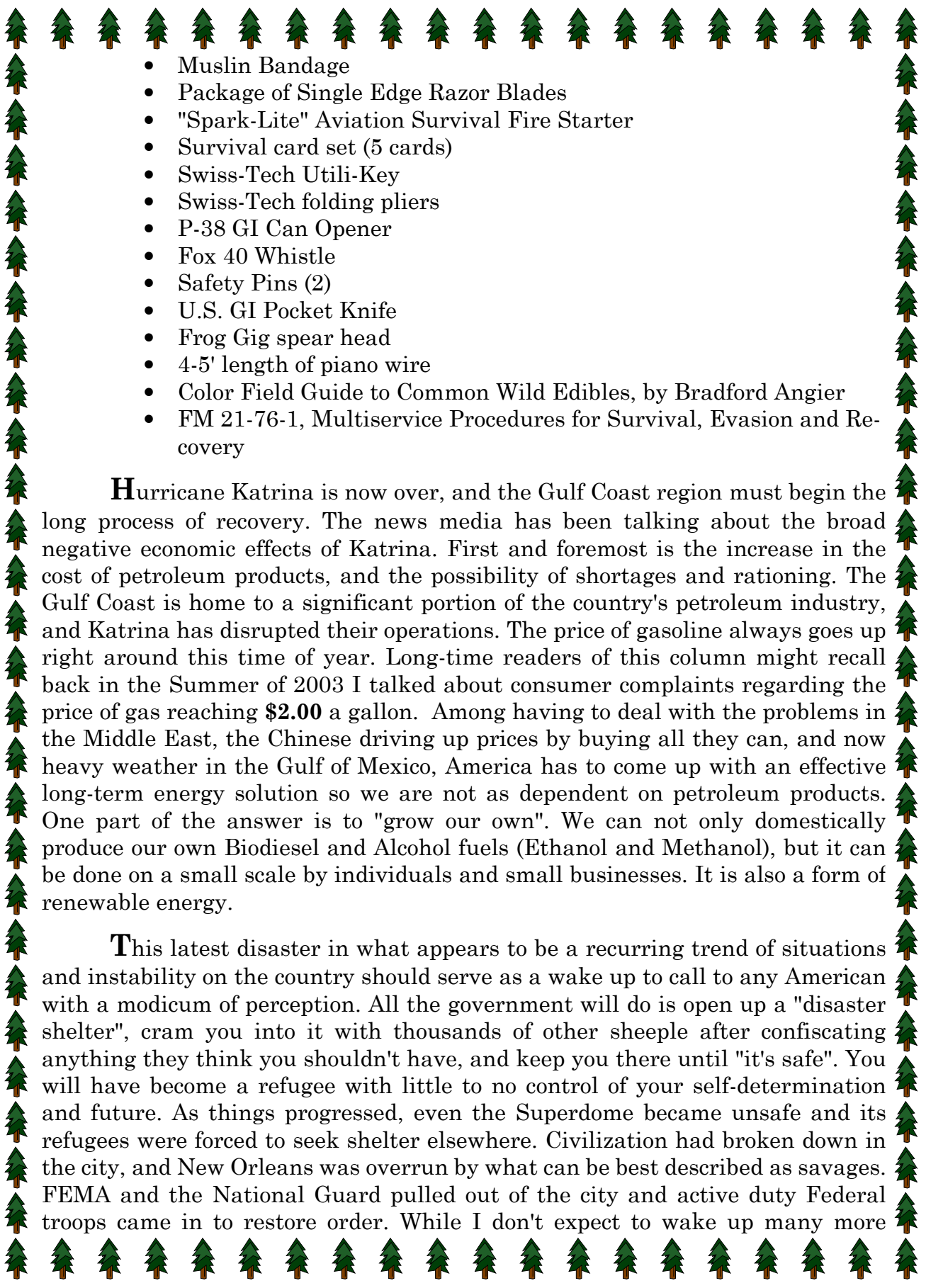
The Pine Tree Journal

"Live free or die; death is not the worst of evils."
- General John Stark, 1728-1822

Autumn is here, and that means hunting season. Whatever game you seek, a small contingency kit is always a useful thing to bring into the field with you just in case your day outing runs into the unexpected. The following is an example of a contingency kit that fits into a small package, and can be placed inside a backpack. It's designed as a general-purpose kit that can be of use in a wide variety of situations and environments. The kit was originally built around a U.S. Military vehicle first-aid kit box, and was later transferred to a [Spec-Ops Brand](#) "Pack-Rat" pack organizer. It contains the following:



- Signal mirror
- [Inova](#) 24/7 light with spare batteries
- Emergency Fishing Kit
- Gill Net
- Magnesium block fire starter
- Space Blanket
- Small Bic Lighter (2)
- Trioxane fuel bar
- Emergency Fishing Kit
- Straw-type water filter
- Mini folding saw with wood and metal blades
- Roll of trip wire
- Dental Floss
- Small Sewing Kit
- Wooden "tongue depressor" wrapped with duct tape, first-aid tape, and electrical tape
- Gauze Pads
- Band-Aids
- Antibiotic Ointment

- 
- Muslin Bandage
 - Package of Single Edge Razor Blades
 - "Spark-Lite" Aviation Survival Fire Starter
 - Survival card set (5 cards)
 - Swiss-Tech Utili-Key
 - Swiss-Tech folding pliers
 - P-38 GI Can Opener
 - Fox 40 Whistle
 - Safety Pins (2)
 - U.S. GI Pocket Knife
 - Frog Gig spear head
 - 4-5' length of piano wire
 - Color Field Guide to Common Wild Edibles, by Bradford Angier
 - FM 21-76-1, Multiservice Procedures for Survival, Evasion and Recovery

Hurricane Katrina is now over, and the Gulf Coast region must begin the long process of recovery. The news media has been talking about the broad negative economic effects of Katrina. First and foremost is the increase in the cost of petroleum products, and the possibility of shortages and rationing. The Gulf Coast is home to a significant portion of the country's petroleum industry, and Katrina has disrupted their operations. The price of gasoline always goes up right around this time of year. Long-time readers of this column might recall back in the Summer of 2003 I talked about consumer complaints regarding the price of gas reaching **\$2.00** a gallon. Among having to deal with the problems in the Middle East, the Chinese driving up prices by buying all they can, and now heavy weather in the Gulf of Mexico, America has to come up with an effective long-term energy solution so we are not as dependent on petroleum products. One part of the answer is to "grow our own". We can not only domestically produce our own Biodiesel and Alcohol fuels (Ethanol and Methanol), but it can be done on a small scale by individuals and small businesses. It is also a form of renewable energy.

This latest disaster in what appears to be a recurring trend of situations and instability on the country should serve as a wake up to call to any American with a modicum of perception. All the government will do is open up a "disaster shelter", cram you into it with thousands of other sheeple after confiscating anything they think you shouldn't have, and keep you there until "it's safe". You will have become a refugee with little to no control of your self-determination and future. As things progressed, even the Superdome became unsafe and its refugees were forced to seek shelter elsewhere. Civilization had broken down in the city, and New Orleans was overrun by what can be best described as savages. FEMA and the National Guard pulled out of the city and active duty Federal troops came in to restore order. While I don't expect to wake up many more

people than those who have already become aware of our country's declining situation, I do hope that the rest of you take this as a sign to intelligently evaluate your contingency plans and existing preparations.

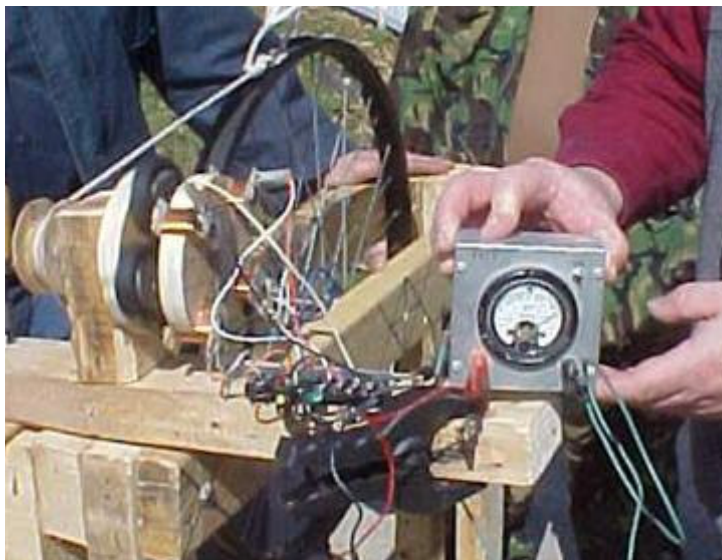
East American Survival Training (EAST) Review

<http://groups.msn.com/EastAmer-SurvivalTraining/>

by Gary L.

16 April 2005 EAST Spring meeting was held with 6 folks attending. Weather was warm and sunny, perfect for solar panels. Gary had a 12 volt 5 watt panel set up charging a 12 Volt, 7 amp gel cell battery. Dave had a very impressive 12 volt 12 watt flexible marine grade solar panel charging a deep cycle marine battery. Neither battery had regulators and it was discussed the need for regulator if a "bank" of solar panels were used to prevent over charging or "cooking" a battery which will greatly reduce battery life.

"Wildflower" designed a generator from "scavenged" parts primarily from a bicycle, microwave ovens, and scrap lumber. Wildflower showed it powering a mini Christmas light bulb (usually 7 watts). I momentarily forgot older basic electronics, and asked how useful this could be as it was obviously low current AC. Wildflower pointed out the 4 LED's (Light Emitting Diodes) served as a rectifier. Diodes were used for rectifiers before IC (integrated circuits) bridge rectifiers. The generator was powered by foot on an adaptation of the old treadle sewing machines. So what would this do besides light up a very small bulb? Wildflower had never put this on a meter but estimated it would put out about 6 volts. A 12 volt in-line meter (automotive meter designed to measure voltage in a working circuit) was connected and generator powered up with no load the meter "pinned" at 14.5 v. max when the bulb was added in the meter dropped



below min 10.5 volts. Wildflower noticed the drive belt had loosened, a quick adjustment and the generator ran at 11.4 v. under load steadily. While the voltage would be choppy and low amperage it would surely charge Ni-cad or NiMH batteries. Had there been time to test, would have liked to try charging a gel cell.

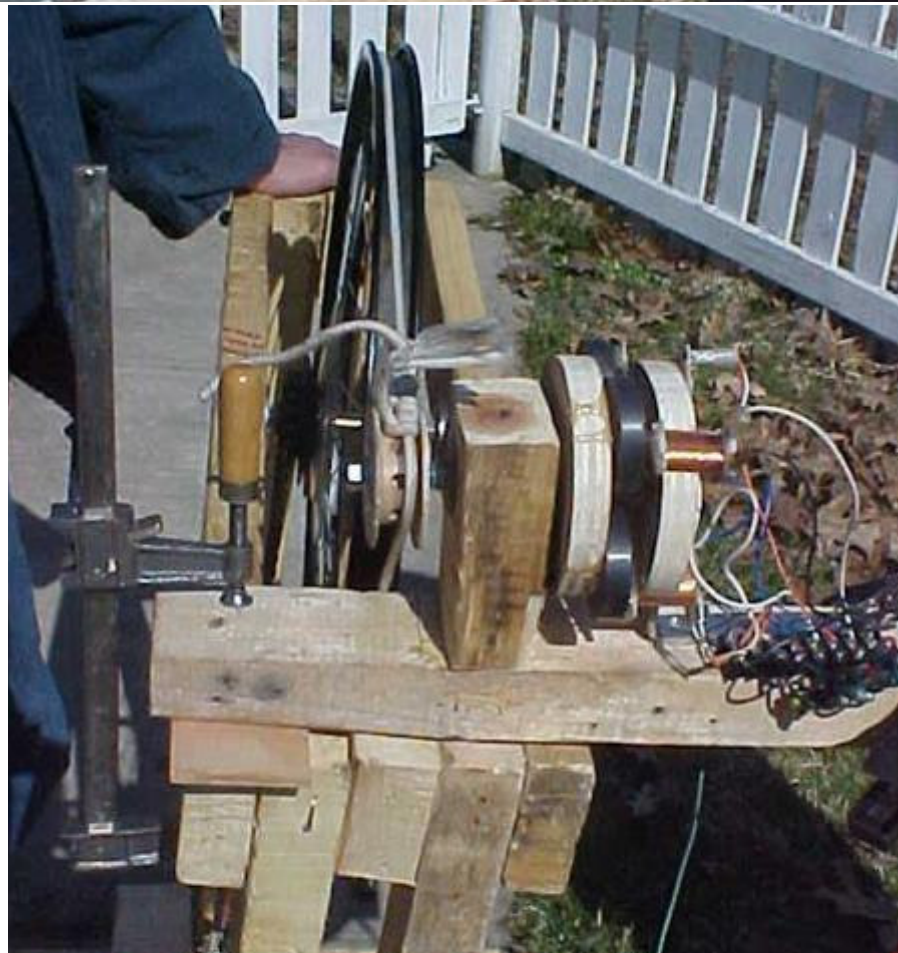
Tom F. then set up a "field radio station/base camp" showing how to make a dipole



antenna by using the proper length wires to an HF radio. He also had VHF radi for operations and a scanner just to monitor. Upon completing the "base camp" perimeter patrol was simulated. Focus was on using numerical codes an operational and tactical frequencies. 3 person patrol the middle person would b



on operational fre and able to talk t "Base camp" whil Point and Ta would be able t talk to each othe. If we needed to tal to middle person, e ther Point woul drop back and tall Or more often whic seemed to work bet er, Point stoppe and to keep propo spacing middle di to. Tail would com up and pass messag to middle.



Finally, w tested a new Isrea Battle wound dress ing. It proved not a simple to work as th instructions ap peared. The wra tore through the cli that was designed t add pressure to th wound and be sel applying. A simila dressing "Blood Stop per" trauma dressin was also shown, : wasn't easily self ap plied but could b done. Then a star dard 5X9 inch steril pad and cravat wa





used, not easily self-applied, but did an effective job. A standard first aid cravat / triangle bandage has a multitude of uses and for space and cost gets my recommendation.

Summer 2005 Meeting: The most important lesson learned at this meeting was intel and info must be up to date. Maps and trail guides had discrepancies that affected the day's plans. I had left my house arriving about 15:30 Fri. (15 July) in the Woodford, Vt area. The plan was to hike the A.T. from the trailhead on Rte. 9. to Little Pond. There is Green Mtn. Natl. Forest Trail # 275, which goes from Rte. 9 at another location to Little Pond that is a dirt road that should be passable by "Jeeps". Since I was solo at this point, I thought I'd do a drive recon in 2WD and would shift into 4X4 mode and get out as the road did look a bit iffy. I passed high-tension power lines and in a bit the road worsened. I scraped bottom a rock was hidden in grass taller than my ground clearance, which was somewhat weighted down by the camper I had on the back. Was going slow so no harm done... A bit further up the road hit bottom again, sheared one of the straps holding the camper on the truck, it also shifted position on the bed of the truck and spilled gear that wasn't secured. Still no harm but road was looking rougher... Decided time to turn around and go to the commercial campground. It was obvious the guide was wrong and we wouldn't be able to





stage a vehicle at Little Pond (might be a worthy 4X4 excursion when better equipped for off roading though).

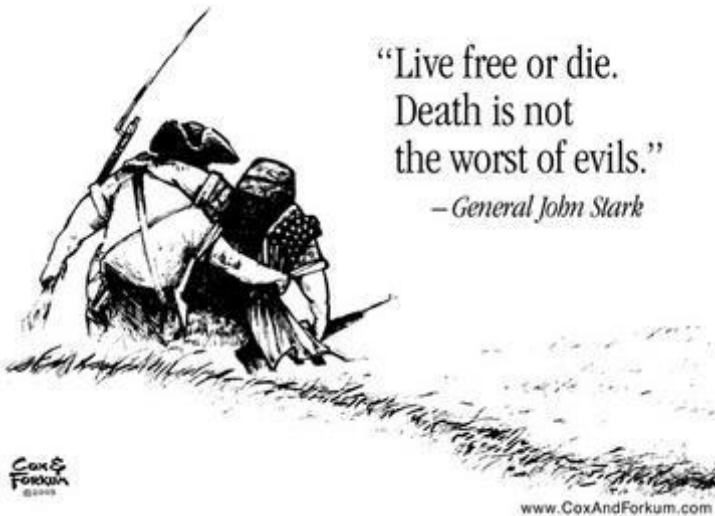
Pine Hollow Campground, a nice little campground, \$28/nite water and electric, hot showers included in price, clean bathrooms, although a bit short on recreational stuff, they did offer wi-fi for computers also included in price. Cost was typical for those in the area. Carleton and Jeffrey B. arrived at camp near dark and "roughed it" in tent camping. Sat. 08:30 (16 July) made our way to the A.T. trailhead parking area ...note on U.S.G.S map dated 1954 revised 1997 shows the parking area to the east of A.T. on Rte. 9 in Woodford, it appears to have been replaced with a runaway truck ramp and the trail parking is just to the west of the A.T...I'd estimate could park at least 40 cars and has bathroom facility.... We reviewed the map and decided that a slight change of plans had to be made as it would be about an 8 mi. hike rather than the 5 mi. hike that was planned on because a vehicle couldn't get to Little Pond. It was decided to leave 1 truck (mine) at the A.T. parking location (with a note and map for any members who may arrive late) and took C.B's truck to the parking area that starts GMNF Trail #275 at 10:00 as I did make in posts that I wanted to start at 10:00 prompt. Started the hike at 10:10 taking a compass bearing of 320 deg. corrected to true north as this area magnetic north is 14.5 deg. to the west. Shortly up the trail we came accross deer tracks and "big cat" tracks. Although I had considered not even packing a gun for this event, I had put a .22 High Standard semi auto pistol in the back pack





which I then strapped on carried in the "gunny sack" which is a fanny pack look a like with a holster inside.

Also along the way we saw a rock that someone got creative and painted to look like a shark. At 10:40 we came to the point where the High Tension electric lines intersected trail #275. We had decided to follow the power lines as we figured the lines hap to be maintained and it looked like a pretty good trail that quads and dirtbikes traveled. SNAKES ALIVE !!! We must have encountered at least 10 mostly the "black racer" variety which is harmless, and they yielded the trail to us quickly, but I still hate snakes. Next problem that delayed our progress was a beaver pond where there was none indicated on the map, there were several small brooks that also weren't indicated but really didn't obstruct our progress much up to this point. At 12:10 we intersected the A.T. Appalachian Trail, confirmed compass bearing of 190 deg. and started hiking the A.T. After about only 5 minutes we met Tom F. He explained he hit more traffic and was just a little late, he started hiking in reverse and figured (correctly) that we would meet. We hiked to the Melville-Nauheim Shelter and had our lunch 12:35 - 13:10. Refreshed we went on the final leg of the trip which was only 3/4 mi. away but the steepest terrain fortunately down hill although Tom had just come up it. Ended the hike at 14:20. Cooled the feet in a brook right at the parking lot. Got Carleton and Jeffrey back to their truck and effectively ended the EAST meeting, but went to a mil. surplus store we had passed just into Bennington from Pownal VT and then to a local restaurant for a bite. All in all a great day to get in some hiking and map and compass practice. Jeffrey is trying to organize a group similar to the recent Minuteman action in AZ (in which he participated) and points out there are many illegals coming over the U.S. - Can. border in this area. A similar exercise might be useful near the border and help border patrol apprehend some. I'd be in favor of trying this and sure can use the exercise. Felt pretty tight in the legs next day.



"Live free or die.
Death is not
the worst of evils."
- General John Stark



Editorial Rants

In case you haven't noticed yet, **The Pine Tree Journal** is now a part of Ticom 'Zine. The combining of the two publications is simply a continuance of the same basic philosophy I've had for the past fifteen years; beginning with the creation of Cybertek. Knowledge in both high tech topics such as computers, electronics, and communications is equally important as low-tech forms of knowledge such as self-reliance and preparedness. This philosophy is espoused by the term "technological survivalism" which was first coined during the 1970s by John Williams of Consumertronics. It was also practiced and advocated by many old-school hackers and phone phreaks during the TAP Magazine era.

Cheshire Catalyst, the last editor of TAP and a fellow veteran, mentioned how phreaks & hackers would be the first ones targeted if the U.S. was ever invaded, because they'd know how to set up underground telecommunications networks ala The Moon Is A Harsh Mistress by Robert A Heinlein <http://cheshirecatalyst.com/sidebar.html#army>. The concept of technological survivalism was also mentioned in Steve Levy's Hackers, regarding the design of Lee Felsenstein's Sol computer:

The Sol reflected Lee Felsenstein's apocalyptic fears, shaped by post-holocaust science fiction, that the industrial infrastructure might be snatched away at any time, and people should be able to scrounge parts to keep his machine going in the rubble of this devastated society; ideally, the machine's design would be clear enough to allow users to figure out where to put those parts. "I've got to design so you can put it together out of garbage cans," Felsenstein once said. "In part because that's what I started from, but mostly because I don't trust the industrial structure--they might decide to suppress us weirdos and try to deny us the parts we need." - Hackers, by Steve Levy, Chapter 12

The in-word for technological survivalism now seems to be "sustainable living". Even techie magazines such as Make: have been getting into it with articles like "Swamp Tech", "Making Biodiesel", and their primer on welding. This is fine with me. Contemporary younger hackers are beginning to embrace the idea of turning off the computer periodically to go play in the real world, there is plenty of room for improvement.

When I first started this journey, I had a far more apocalyptic view of the future than I do now. Fifteen years of life experience, a spouse, and a child tend to do that to you, as does witnessing increasing numbers of people who decide to:

- ◆ Practice self-reliance hobbies in one form or another.
- ◆ Buy an old diesel car or truck, and homebrew their fuel out of used vegetable oil.
- ◆ Decide to not vote for a Demopublician or Reublicrat, and instead vote for one of the alternative parties.
- ◆ Set up one of the many little sub-communities of like-minded individuals that have

sprung up everywhere from converted factories in cities (lofts), to old farms.

- ◆ Set up free "WiFi" wireless Internet access nodes.
- ◆ Run personal fabrication set-ups.
- ◆ Promote "open source" operating systems such as Linux and BSD.
- ◆ Put their homes "off the grid" with alternative energy set-ups.
- ◆ Become "guerrilla capitalists".
- ◆ Home school their children, or set up private schools for the families of like-minded individuals.

Why should these actions be considered important, and what do they accomplish?

- ◆ They increase individual independence and self-reliance.
- ◆ They reduce dependence on outside infrastructure.
- ◆ They increase the security level of the country by reducing its vulnerability to disruption by attacks by hostile entities.
- ◆ They promote tightly knit communities.
- ◆ They help protect the country from internal take-over by totalitarian elements.
- ◆ They can help institute positive change in society.

All of this is good, as the end result is a much better country in which to live.

Rome didn't fall in a day and if the United States ever does "collapse" the process will be as long and drawn out as the fall of Rome. Nevertheless, everything didn't totally go away when Rome collapsed. Even today, a good portion of Ancient Rome's transportation infrastructure is still being used. The United States has a rich and extensive technological infrastructure. If we ever have a TEOTWAWKI-type situation in this country, much of it will probably still be intact. The reclamation and restoration of that infrastructure will definitely be possible by groups of prepared technological enthusiasts. This can mean the difference between being set back decades versus centuries.

Whether we are heading towards an eventual collapse, or simply reaching the low-point in a cycle, the country is continually becoming increasingly unstable as time goes on, and no one is immune from it. Many more Americans are going to feel the effects in the future. Those with the foresight to realize what is going on and make the proper preparations will be those who will avoid the brunt of the mess. Maybe if we get enough people to become aware and act accordingly, we can avoid the mess altogether. That's what I would like to see.

