

90. > I've been asked to help in a case where an agent obtained a search warrant
91. > based upon a P2P investigation in which a semi-static IP (cable) was traced
92. > to the suspect's account. Prior to the search, no one swept the area for a
93. > wireless signal, but that's not unusual. The defense points out that the
94. > suspect could have had a wireless network linking any number of machines to
95. > a router and ultimately the cable modem. True. More importantly, they claim
96. > that anyone could have accessed the modem through a hijacked signal, used
97. > the suspect's IP, employed LimeWire to offer c-p, and have led the agents to
98. > the right account, but wrong location. In sum, the defense states that the
99. > SW application was misleading for not pointing out those possibilities, and
100. > that there really wasn't PC to search the home.

101. >
102. > This seems kind of straightforward, but maybe I'm naive. Regardless,
103. > suggestions are always helpful. It seems to me that the bottom line is that
104. > you can't prove a negative. Martians could have hijacked the IP. I'd argue
105. > that we knew that the homeowner had the account. We also knew that the
106. > cable access is physically connected to the house. So, I think there's PC
107. > to search the house, as it's very likely that a computer inside the house
108. > accessed the Net through the modem (IP). Still, we've all heard of cases in
109. > which a signal was in fact stolen leading to a search of the wrong computer.
110. > There's also the argument that an unencrypted access point is asking for
111. > trouble. If the defense argument flies, should it be a practice to sweep
112. > for signals (not capturing content) before applying for any SW based on
113. > traced an IP? Even that isn't fail safe. Thanks.

114. >
115. > Jimmy Weg, CFCE
116. > Agent in Charge, Computer Crime Unit
117. > Montana Division of Criminal Investigation
118. > 2225 11th Ave.
119. > Helena, MT 59601
120. > 406.444.6681
121. > 406.439.6185 (cell)
122. > jweg@mt.gov

123. >
124. --
125.