Effective Incident Handling Is A Requirement For Security

C. Matthew Curtin, CISSP
Interhack Corporation

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Conflict of Interest

C. Matthew Curtin, CISSP
has no real or apparent conflicts of interest to report.

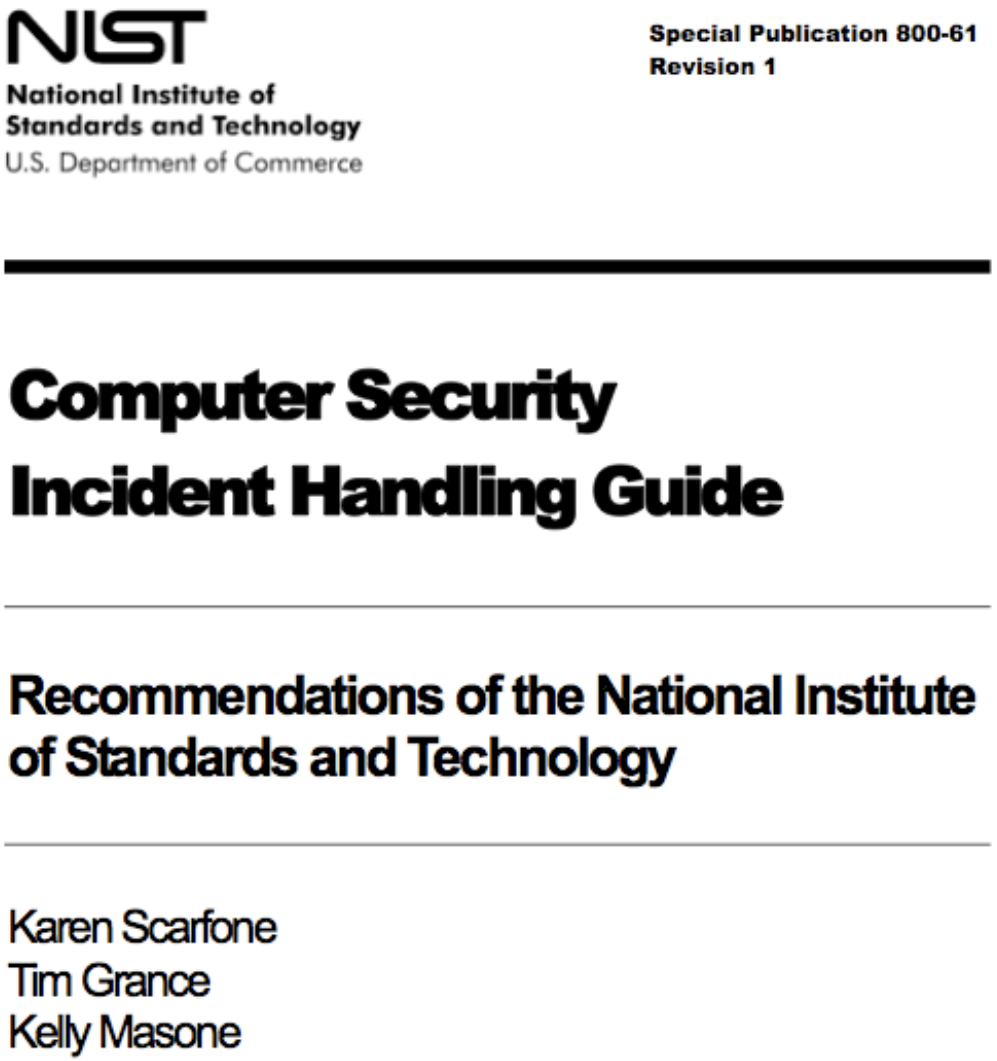
What We Hope to Learn Today

1 When to declare an incident
2 Phases of a security incident
3 How organizations should develop capability
4 How to maintain readiness

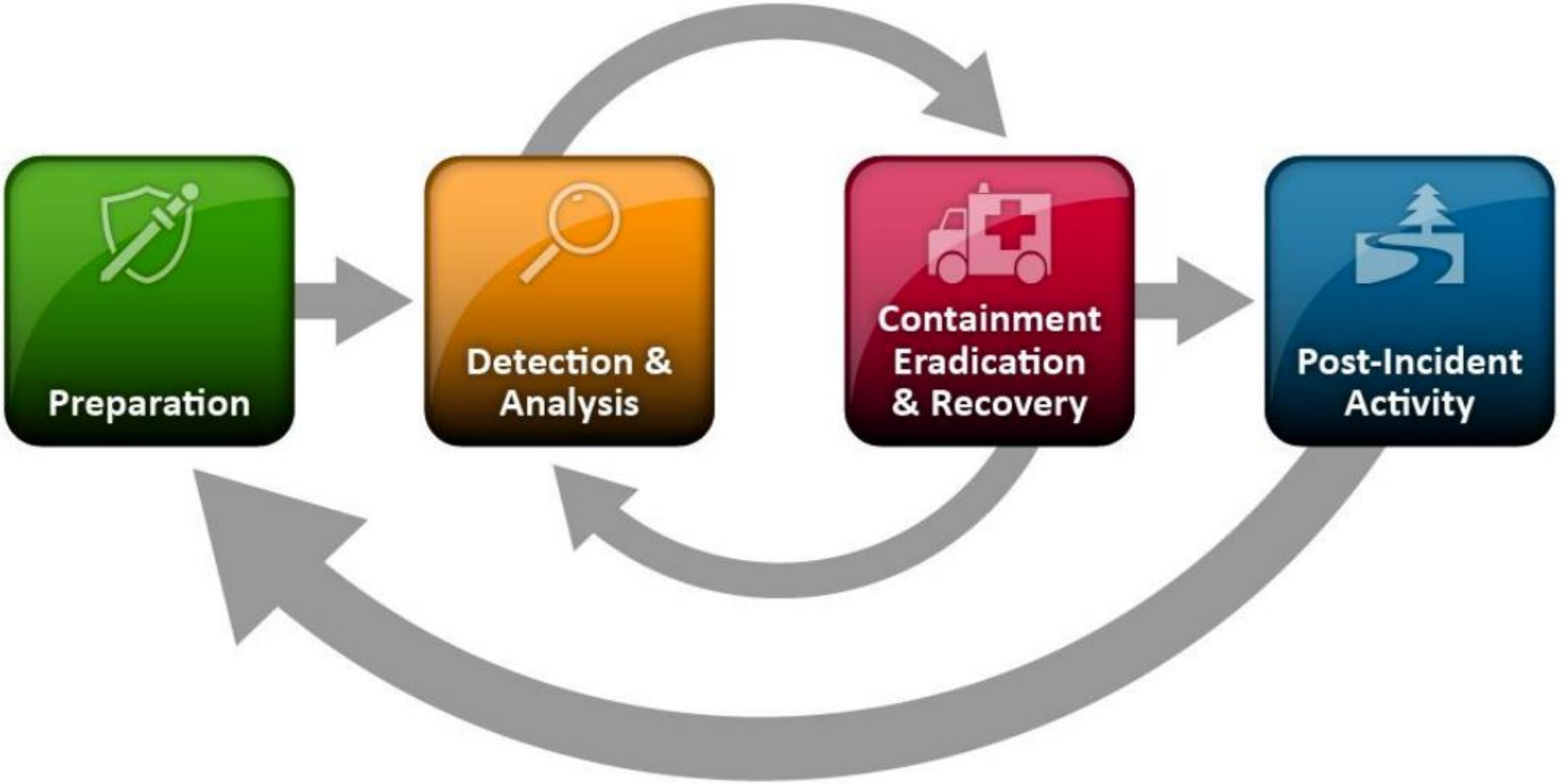
What is an "Incident?"

"a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

—NIST SP 800-63

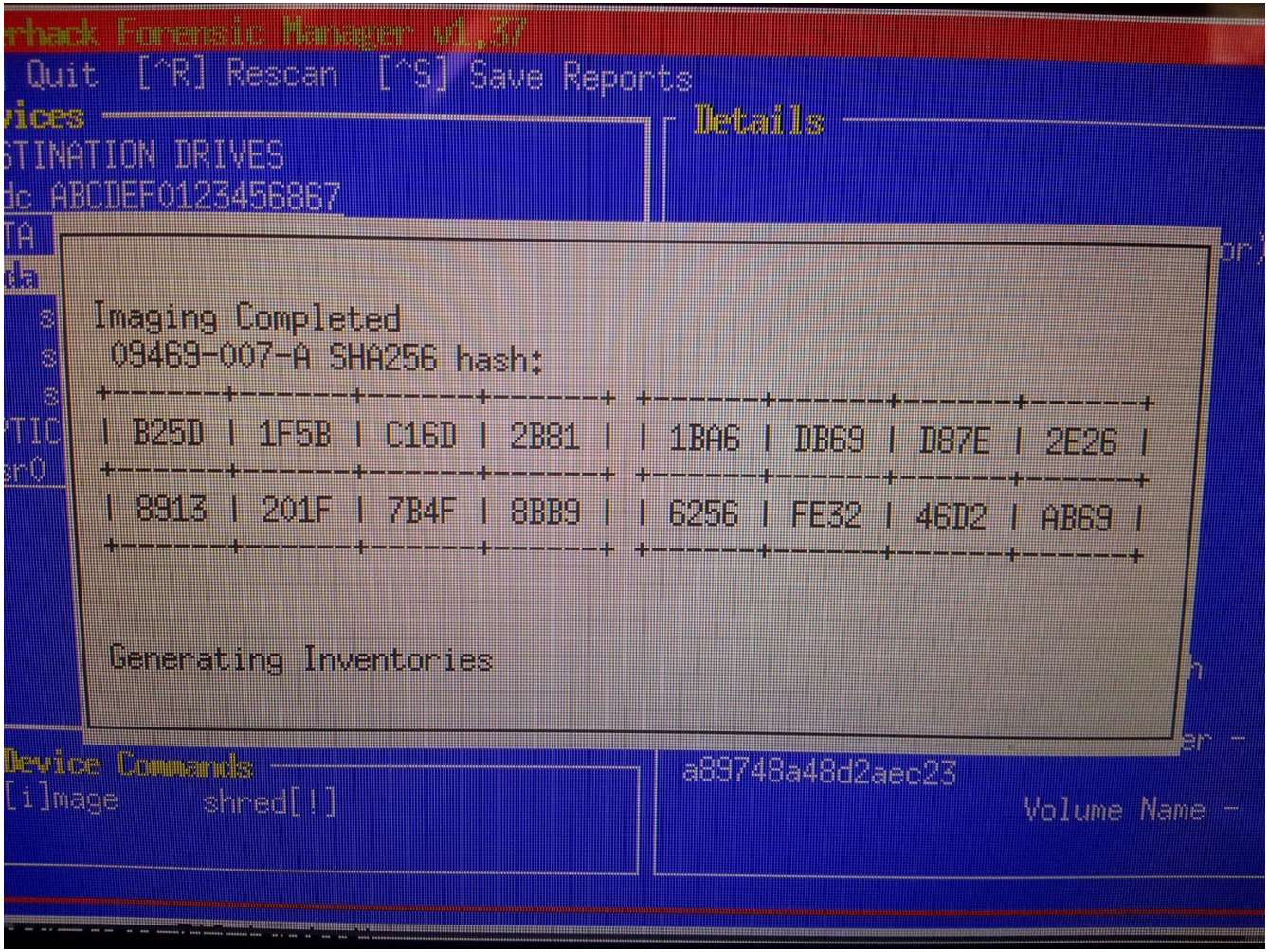


Phases of an Incident



Preparation

Preparation



Preparation

Detection and Analysis

```
496e 7465 7240 6374 6976 6520 5061 6765 Inter@ctive Page
7220 4261 636b 7570 2f52 6573 746f 7265  r Backup/Restore
2046 696c 650a 0200 5c00 1800 4c6f 6361   File...\...Loca
7469 6f6e 2042 6173 6564 2053 6572 7669  tion Based Servi
6365 7300 0900 4175 746f 5465 7874 0016  ces...AutoText..
0041 7574 6f54 6578 7420 4461 7461 2056  .AutoText Data V
6572 7369 6f6e 0013 0048 616e 6468 656c  ersion...Handhel
6420 4b65 7920 5374 6f72 6500 0e00 5047  d Key Store...PG
5020 4b65 7920 5374 6f72 6500 0d00 5365  P Key Store...Se
7276 6963 6520 426f 6f6b 0019 0044 6566  rvice Book...Def
6175 6c74 2053 6572 7669 6365 2053 656c  ault Service Sel
6563 746f 7200 1200 5472 7573 7465 6420  ector...Trusted
4b65 7920 5374 6f72 6500 1700 4861 6e64  Key Store...Hand
6865 6c64 2043 6f6e 6669 6775 7261 7469  held Configurati
6f6e 000f 0048 616e 6468 656c 6420 4167  on...Handheld Ag
```

Detection and Analysis

Offset	*Responsive Record*
20958	mapi://{S-1-5-21-584965487-2¬ 563626095-4050862279-1301}/¬ badboy@newcompany.com($bd61f¬ 120)/0/Deleted Items/
22e3a	Solid Fuel Calculation Formula V.1.1.xlsx
31494	mapi://{S-1-5-21-584965487-2¬ 563626095-4050862279-1 badboy@newcompany.com(120)/0/Deleted Items/
3159a	Solid Fuel Calculation V.1.1.xlsx
404b8	mapi://{S-1-5-21-58496 563626095-4050862279-1 badboy@newcompany.com(120)/0/Inbox/
405ae	Solid Fuel Calculation V.1.1.xlsx
41f26	mapi://{S-1-5-21-58496 563626095-4050862279-1 badboy@newcompany.com(120)/0/Inbox/
4201c	Solid Fuel Calculation V.1.1.xlsx
48f50	mapi://{S-1-5-21-584965487-2¬ 563626095-4050862279-1301}/¬ badboy@newcompany.com($bd61f¬ 120)/0/Deleted Items/
49056	Solid Fuel Calculation Formula V.1.1.xlsx

Figure 4: Search Results for Filename Solid Fuel Calculation Formula V.1.1.xlsx in MSS802FF.log

Offset	*Responsive Record*
20958	mapi://{S-1-5-21-584965487-2¬ 563626095-4050862279-1301}/¬ badboy@newcompany.com($bd61f¬ 120)/0/Deleted Items/
22e3a	Solid Fuel Calculation Formula V.1.1.xlsx

Detection and Analysis (FRE 702)

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

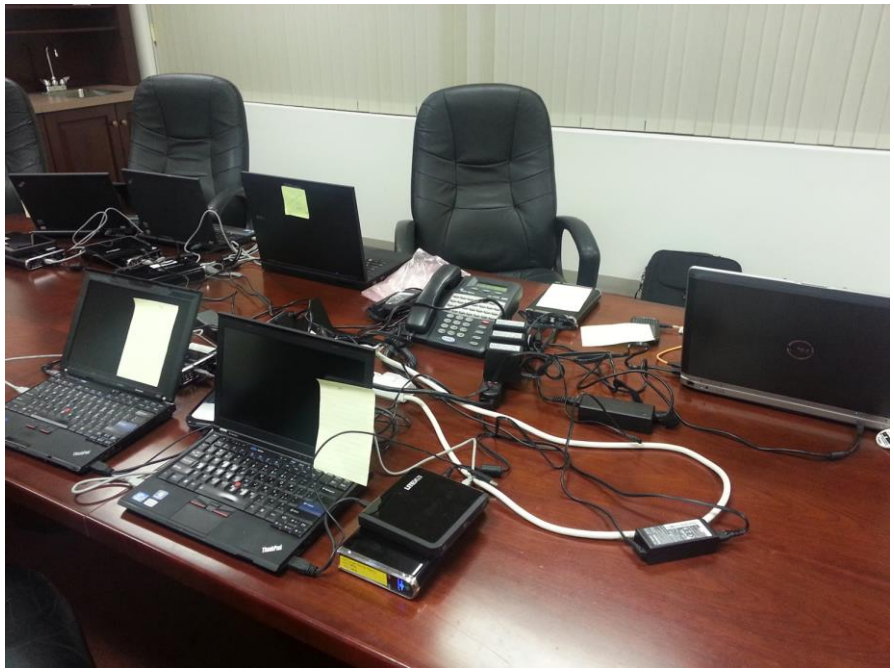
(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

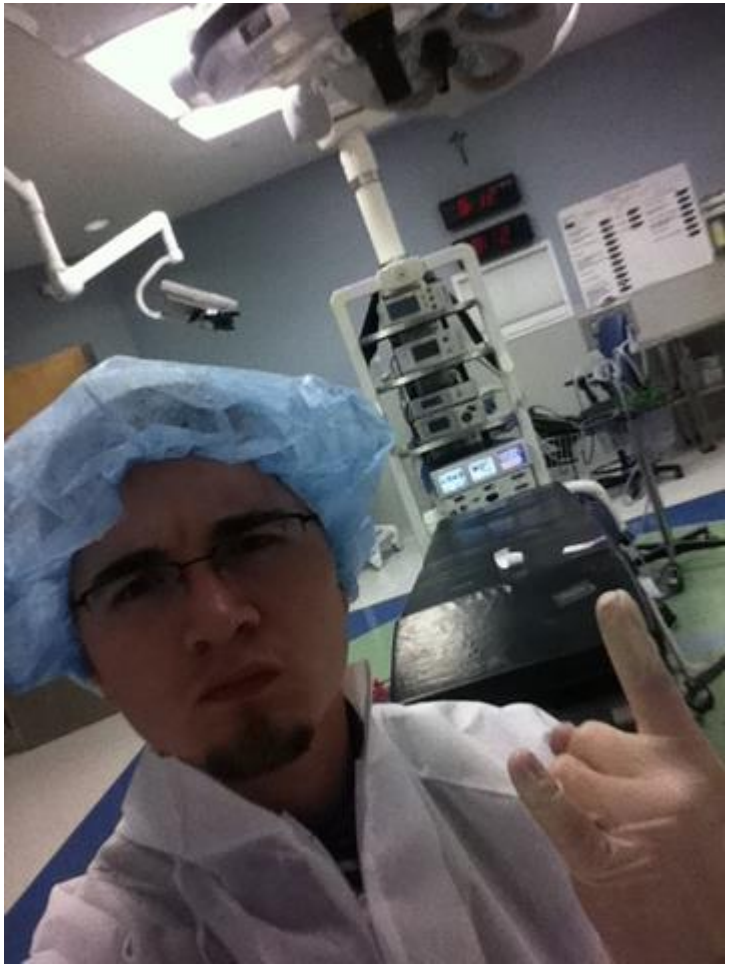
(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.

Containment, Eradication & Recovery



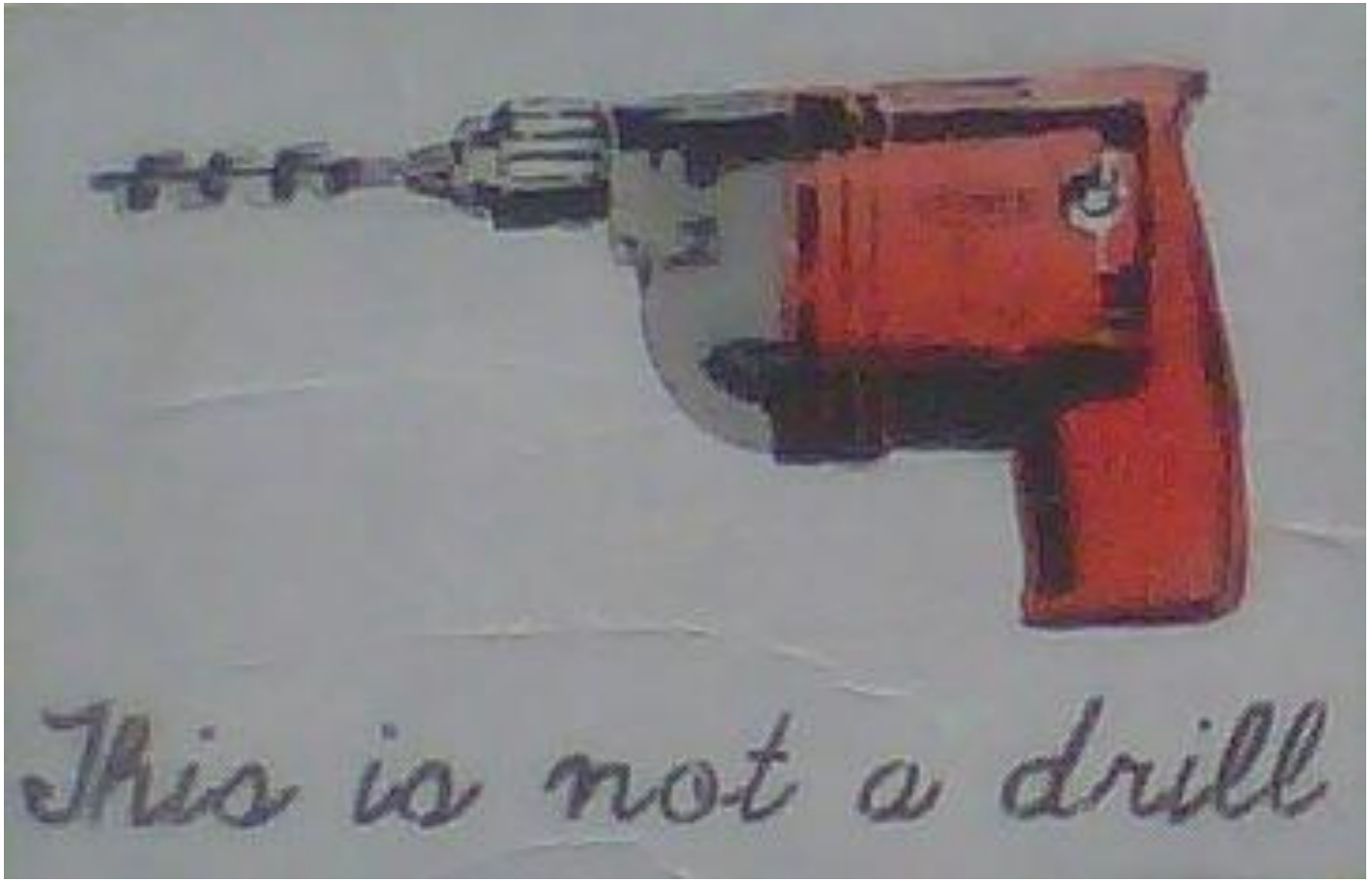


Containment, Eradication & Recovery

Post-Incident Activity

Developing Capability

Maintaining Capability



Questions?

C. Matthew Curtin, CISSP
Interhack Corporation
5 E Long St 9th Fl
Columbus, OH 43215

cmcurtin@interhack.com

INTERHACK

HIMSS CENTRAL & SOUTHERN OHIO Chapter